Fall November 20, 2019

Obstacles to Transatlantic Harmonization of Data Privacy Law in Context

W. Gregory Voss

OBSTACLES TO TRANSATLANTIC HARMONIZATION OF DATA PRIVACY LAW IN CONTEXT

W. Gregory Voss†

Abstract

Globalization seems to call for the harmonization of laws, especially in sectors affecting global business, and this is all the truer with respect to laws affecting the technology industry, with the facility of its cross-border communications networks. Data privacy law on both sides of the Atlantic benefits from common origins but eventually divergence occurred, causing compliance challenges for companies and the potential halting of cross-border data flows from the European Union to the United States. Harmonization could possibly obviate such difficulties, and there is a window of opportunity to achieve this with discussion in the United States of a potential federal data privacy law.

After setting out the historical context, this study posits and details three major obstacles to full-scale transatlantic harmonization of data privacy law, from the perspective of what has become the predominant data privacy model—that of the European Union. These are: laissez-faire policy and neoliberalism in the United States (and resulting focus on self-regulation there), the lobbying power of the U.S. technology industry giants in a conducive U.S. legislative system, and differing constitutional provisions on both sides of the Atlantic. Each of these elements makes attaining true harmonization more difficult, if not impossible. Nonetheless, corporate action in the United States might have given some hope of a de facto harmonization of practices, although hopes have not led to the equivalent of harmonization of laws. Political and other realities provide further context, leaving reason to be doubtful about the prospects of true

† Associate Professor in Business Law, TBS Business School (Toulouse, France). The author is Associate Member of IRDEIC – Research Institute in European, International and Comparative Law, a Jean Monnet Centre of Excellence, Toulouse 1 Capitole University, and a member of the Board of Directors of the French Academy of Legal Studies in Business (AFD&M). He is a graduate of Toulouse 1 Capitole University (D.E.S.S. (Master 2) *Droit et systèmes d'information* (Law and Information Systems), 2001), the University of Michigan Law School (J.D., 1983), and Georgetown University School of Foreign Service (B.S.F.S., 1980). The author may be reached at g.voss@tbs-education.fr. This study has been adapted from a paper the author presented at the University of Pennsylvania Law School *Journal of Business Law* 2019 Symposium on Harmonizing Business Law held in collaboration with the University of Maryland Center for the Study of Business Ethics, Regulation & Crime (C-BERC) on January 26, 2019, in Philadelphia. The author would like to thank the *University of Illinois Journal of Law, Technology & Policy* (*JLTP*) peer reviewers for their helpful comments, and the *JLTP* editors, members, and staff for their assistance during the editing process.

transatlantic harmonization of data privacy law. Finally, certain areas for improvement in the context of U.S. legislative action are discussed.

TABLE OF CONTENTS

INTRODUCTION

Three events that occurred in 2018 helped to catalyze the interest of Americans and their legislators in their nation's data privacy law: first, the Cambridge Analytica incident, which came to light in spring 2018, where Facebook user data were scraped for use by Cambridge Analytica to influence

the 2016 U.S. presidential election;[1] second, through comparison with it, the entry into application in May 2018 of a regulation that resulted from years of work on data privacy legislative reform in the European Union—the General Data Protection Regulation;[2] and finally, a month later, the passage of the California Consumer Privacy Act of 2018 (CaCPA), a state law which will offer the most stringent U.S. data privacy protections when it takes effect in 2020.[3] The ensuing political atmosphere, where there have been calls for legislative action at the federal level in the United States, may be seen as a window of opportunity for the adoption of data privacy legislation in the United States[4] that could potentially result in the harmonization of American domestic law,[5] if not transatlantic data privacy law harmonization. But what are we speaking about when we discuss harmonization of law, generally? In technology law; and more narrowly, in data privacy law?

Harmonization has been described as entailing "the adoption of a single and uniform norm for all participating jurisdictions concerned," and as having as a result the creation of a level playing field, removing barriers to trade.[6] The jurisdictions involved in the harmonization of laws may be federal ones (such as U.S. states), regional ones (such as the member states of the European Union), or more broadly international ones. However, in the context of digitized information, one must keep in mind that that the use of the international communications network known as the World Wide Web (through which much of such data transit) is, well, *worldwide.* Communications, in turn, have played

1. Indeed, the Cambridge Analytica incident resulted in the "global conversation around data privacy" changing dramatically, with Washington spending most of 2018 "talking tough to tech companies and threatening a crackdown on the wanton collection, dissemination, and monetization of personal data." *See* Issie Lapowsky, *Get Ready for a Privacy Showdown in 2019*, WIRED (Dec. 27, 2018 07:00 AM), https://www.wired.com/story/privacy-law-showdown-congress-2019/. For a general discussion on the Cambridge Analytica revelations *see, e.g.*, Dr. Iga Kozlowska, *Facebook and Data Privacy in the Age of Cambridge Analytica*, HENRY M. JACKSON SCH. OF INT'L STUD., U. WASH. (Apr. 30, 2018), https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/.

2. Former European Data Protection Supervisor Giovanni Buttarelli is reported to have referred to "geopolitical pull, with privacy regulation rising up the political agenda outside Europe," as well as noting "a new appetite for a federal law" in the United States, following the application of the General Data Protection Regulation. *See* Natasha Lomas, *Europe Is Drawing Fresh Battle Lines Around the Ethics of Big Data*, TECH CRUNCH (Oct. 3, 2018), https://techcrunch.com/2018/10/03/europe-is-drawing-fresh-battle-lines-around-the-ethics-of-big-data/.

3. *See* Anupam Chander et al., *Catalyzing Privacy Law* (U. of Col. Legal Studies Research Paper No. 19-25, 2019), at 3–4, https://ssrn.com/abstract=3433922 (referring to the CaCPA as evidence that "California has emerged as a kind of privacy superregulator, catalyzing privacy law in the United States.").

4. The American Civil Liberties Union's senior legislative counsel commented in an op-ed piece that the private sector reckoned "with the fact that there's popular momentum for federal privacy legislation following revelations of Cambridge Analytica's misuse of Facebook data." *See* Neema S. Guliani, *The Tech Industry Is Suddenly Pushing for Federal Privacy Legislation. Watch Out.*, WASH. POST (Oct. 3, 2018), https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html.

5. This could happen through the Trump administration's desire for a bill to "harmonize the regulatory landscape" and through proposals for a federal law that would "preempt any statewide legislation." *See* Lapowsky, *supra* note 1.

6. *See* Thomas Cottier, *Technology and the Law of International Trade Regulation in* THE OXFORD HANDBOOK OF LAW, REGULATION, AND TECHNOLOGY 1017, 1028 (Roger Brownsword et al.eds., 2017) (referring to technology law, including technology regulation and standards, which may serve as technical barriers to trade, although the author cites other areas where "regulatory convergence" may occur: IP standards, competition law, or rules of liability).

a role in the "deepening of economic globalization."[7] However, globalization does not merely have economic effect: it also has an impact on social and cultural relations.[8] Furthermore, economic globalization seems to call for a global legal framework.[9] According to one Nobel-Prize-winning economist, international legal frameworks are necessary in order for the global economy to function smoothly.[10]

No single international legal framework exists governing internet communications. This was clear when a U.S. lawyer advised colleagues to think beyond boundaries in 1994—early in Internet history.[11] Lawyers were to keep the laws of other jurisdictions in mind, when practicing their profession.[12] However, divergence in internet governance still reflects cultural and legal differences today, and leaders of Japan, South Africa, China and Germany have been cited as calling for "global oversight of the tech sector," without specifically mentioning data privacy or agreeing on governance architecture.[13] This divergence is also evidenced when comparing laws in the United States, where the government has been broadly deferential to the tech sector and has placed few restrictions on data use, and those in the European Union, where greater limits on such use have been imposed.[14]

Harmonization of technology law has mainly been achieved in the European Union.[15] This is also the case for data privacy, or in the European Union, "data protection" legislation, as has been reinforced by the adoption of the EU's General Data Protection Regulation ("GDPR"),[16] which became

7. *See* JARED N. BHAGWATI, IN DEFENSE OF GLOBALIZATION 4 (2007).

8. *See, e.g.*, JAN KLABBERS, INTERNATIONAL LAW 17 (1st ed. 2013).

9. *See id*.

10. JOSEPH E. STIGLITZ, MAKING GLOBALIZATION WORK 207 (2006) ("Eventually, we should be working toward the creation of international legal frameworks and international courts—as necessary for the smooth functioning of the global economy as federal courts and national laws are for national economies.").

11. "The Internet has shrunk the world. True, it has brought the people of the world closer in many respects. In doing so it is also exposing our cultural and legal differences and our different views of how the world should operate. It will continue to expose the fissures between different governments and people. The point is that the Internet knows no geographical boundaries. Your thinking should not have geographical boundaries, either." *See* RAYMOND L. OCAMPO JR., SURFING THE LAW AND TECHNOLOGY TSUNAMI 39 (2001) (reproducing the text from a keynote address to the California State Bar Convention on Sept. 23, 1994).

12. *Id*. at 38.

13. *See* Keith Bradsher & Katrin Bennhold, *World Leaders at Davos Call for Global Rules on Tech*, N.Y. TIMES (Jan. 23, 2019), https://nyti.ms/2S7kfic (noting that this call for global governance is set against the backdrop of geopolitical stakes such as U.S. leadership of the tech industry, Chinese unwillingness to accept limits on government access to personal data, and a U.S.-China dispute over telecommunications giant Huawei).

14. *See id*.

15. Cottier, *supra* note 6, at 2028.

16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]. In addition to the twenty-eight member states of the European Union, the GDPR has been incorporated into the European Economic Agreement (EEA) Agreement and so applies to the three European Free Trade Association (EFTA) EEA states—Iceland, Liechtenstein, and Norway. Press Release, EFTA, General Data Protection Regulation incorporated into the EEA Agreement (July 6, 2018), http://www.efta.int/EEA/news/General-Data-Protection-Regulation-incorporated-EEA-Agreement-509291. Readers should keep this fact in mind. Nonetheless, this study will continue to refer to the European Union when discussing the GDPR and transatlantic harmonization. For a discussion of the main provisions of the GDPR, *see generally* W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting*, 72 BUS. LAW. 221 (2016).

applicable on May 25, 2018.[17] The terminology itself is not harmonized and data protection is a broader term in some respects than privacy.[18] From a comparative perspective, the EU concept covers more processing activities, data security, and data subject rights than the traditional U.S. concept of "information privacy."[19] That term arose as a concept in the 1960s and 1970s.[20] Professor Lee A. Bygrave also points out the differences between "data privacy" and "privacy," while retaining the former term as a synonym of "data protection," and employing it in the title of a book covering EU data protection law.[21] Data protection and privacy are similar, but different legal concepts, as pointed out by Professor Christopher Kuner.[22] Similarly, Professor Graham Greenleaf comments as follows about certain differences:

> the concept of "data protection" (or "data privacy," which is the term used in this book) is now relatively well defined as a set of "data protection principles," which include an internationally accepted set of minimum principles plus additional principles which are evolving continually through national laws and international agreements. "Privacy" also encompasses aspects of physical privacy which are not part of data privacy. In addition, "data privacy" laws only apply to data processing that occurs outside the sphere of family and personal affairs, where "privacy protection" is not so restricted.[23]

Thus, this study does as Kuner and Greenleaf did, and more generically uses the term "data privacy" throughout, which seems less-Eurocentric and more "neutral" than "data protection" and may therefore be seen as a kind of compromise position, to indicate protection for what is called "personally identifiable information" or "PII" in the United States, and "personal data," a broader term than PII,[24] in the European Union, although it is understood that these choices may lead to criticism.

---

17. GDPR, *supra* note 16, at art. 99(2).

18. The term "data protection" in the European Union translates a concept that is broader in certain respects than "privacy." This is briefly discussed in Part II.C.

19. *See generally* STEVEN CHABINSKY & F. PAUL PITTMAN, THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: USA: DATA PROTECTION 2019 (2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (detailing legal treatment of data protection in the United States).

20. *See* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 8 (2006). (showing Bennett and Raab commenting that "Over time, it became clear that the European concept of *data protection* was being used in much the same way as the term *information privacy*).

21. *See* LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 3 (1st ed. 2014) ("Data privacy (or data protection) is also not fully commensurate with privacy, at least if the latter is defined in terms of non-interference, limited accessibility, or information control" (citation omitted)). Some, however, see the term "data protection" as overly technical and concentrating on the *data* rather than the *person* as the object of protection." *Id*. at 11 (citation omitted).

22. "Strictly speaking, data protection law, which restricts the processing of data relating to an identified or identifiable person, and grants persons rights in the processing of data relating to them, is closely related to, but distinct from, the concept of 'privacy.'" Christopher Kuner, *The European Union and the Search for an International Data Protection Framework*, 2(2) GRONINGEN J. INT'L L. 55 n.1 (2014), http://www.kuner.com/my-publications-and-writing/untitled/kuner-groningen-journal-von.pdf.

23. GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE & HUMAN RIGHTS PERSPECTIVES 5 (2014).

24. For a recent discussion of the differences between PII and personal data, *see* W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*,

However, not only does the data privacy law (to the extent it exists) of the United States not conform to that of the European Union,[25] it is not harmonized within the borders of the fifty states,[26] and it "seems stuck," as no meaningful new privacy laws had been enacted in the United States within more than a decade, according to one commentator writing in 2015.[27] Lack of harmonization, however, may bring compliance costs to firms. For example, when the European Commission (Commission) first proposed the GDPR in 2012, one of its arguments for such legislation was the need for greater harmonization of EU member state law, and it calculated that having only one law instead of 27 member state laws to comply with (Croatia was not yet an EU member state then, but the United Kingdom was still one) would bring savings to firms—which, when coupled with the elimination of filing and other administrative requirements, was estimated at €2.3 billion.[28] In a submission to the National Telecommunications and Information Administration (NTIA), the Head of the International data flows and protection Unit of the Commission's Directorate for Fundamental rights and rule of law, within the General Justice and Consumers Directorate, highlighted that, "companies increasingly operate across borders and prefer to apply a single set of rules in all of their business operations worldwide" so that having the United States adopt an international instrument, such as Convention 108 (discussed in Part I.A.3), "would help commercial operators navigate between different legal systems and offer new opportunities to further trade."[29] Furthermore, lack of harmonization may lead to other problems, such as cross-border data transfer restrictions, which are discussed in Part I.C.

---

56 AM. BUS. L.J. 300–24 (2019). For an earlier view, *see generally* Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877 (2014).

25. It has been recognized that U.S. data privacy law does not provide an "adequate" level of data protection, in the sense of the GDPR's requirement of a determination of such level in order to export personal data from the European Union to a recipient country outside of the European Union. *See* GDPR, *supra* note 16, at art. 45(1). In contrast to the European Union's omnibus data protection regulation, "the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation." *See* U.S. DEP'T OF COMMERCE. EU U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES ISSUED BY THE U.S. DEPARTMENT OF COMMERCE, principle I(1), https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg. The Privacy Shield is discussed briefly in Part I.C.

26. As an example, Solove and Schwartz show the disparity in what is covered by state data breach notification statutes—one element of data protection covered in the European Union by a single piece of legislation, the GDPR. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 2017 205–213 (4th ed. 2017). Furthermore, the adoption of California's Consumer Privacy Act of 2018, at this stage considered unique in the United States, may be seen as further evidence of such disparity. *See infra* Part II.B.3.

27. Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1127 (2015). Professor Daniel Solove echoes this view, pointing out that, while in "the 1970s through the end of the 1990s, the US Congress passed a large number of important privacy laws . . . [a]fter 2000, however, the activity slowed down significantly. On the whole, the U.S. federal legislative activity in the 21st Century is not particularly notable." *See* Daniel Solove, *The U.S. Congress Is Not the Leader in Privacy or Data Security Law*, TEACHPRIVACY (Apr. 9, 2017), https://teachprivacy.com/us-congress-is-not-leader-privacy-security-law/.

28. *See* Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses, European Commission Press Release IP/12/46 (Jan. 25, 2012).

29. Letter from Bruno Gencarelli, Head of Unit, Unit C.4: International data flows and protection, Directorate C: Fundamental rights and rule of law, European Commission to Andrew Redl, Assistant Secretary, National Telecommunications and Information Administration, U.S. Department of Commerce (Nov. 9, 2018), https://www.ntia.doc.gov/files/ntia/publications/letter-docket_no._180821780-8780-01.pdf.

While elements of privacy law itself have been seen to constitute an obstacle by international trade scholars,[30] international harmonization of data privacy law, which would benefit international trade in a globalized world, faces several obstacles.[31] This study aims to engage the topic of obstacles to harmonization of a relatively recent area of business law—data privacy—in context, positing three main obstacles.[32] Although recent, this area of law is nonetheless important because of the economic value of data.[33] As a consequence, the choice has been made in terms of methodology to conduct this study's analysis based on the two large players in Western trade—the United States and the European Union, in part because of the importance of the trade relationship between them,[34] and the important role of data in such transatlantic trade.[35] In addition, the two trade partners represent two divergent models, as will be shown in Part I.B, making them of significance beyond their borders. Furthermore, although there were 134 countries with data privacy laws in April 2019,[36] the impact of EU law on many of these laws (outside of Europe) has been great[37] and will continue to be so with the GDPR.[38] Thus, focusing on EU law, which may be used to a certain extent as a proxy for laws adopted following

30. *See, e.g.*, Nir Kshetri, *Cybersecurity's Effects on International Trade and Investment* in THE QUEST TO CYBER SUPERIORITY (2016) (referring to restrictions of cross-border transfers of personal data to countries without adequate data protection as direct host-country-initiated barriers to international trade for US companies and direct home-country-initiated barriers to international trade for EU companies).

31. *Id.*

32. *See infra* Part II & III.

33. Indeed, Nobel-prize-winning economist Jean Tirole states that "The processing of data will perhaps be the main source of value added in the future." JEAN TIROLE, ECONOMICS FOR THE COMMON GOOD 405 (Steven Rendall trans., Princeton University Press, 2017). As an example, a European Data Market study commissioned by the European Commission has measured the overall impact of the data market on the EU economy as approximately €300 billion in 2016 and increasing to €739 billion in 2020. *Final results of the European Data Market Study Measuring the Size and Trends of the EU Data Economy*, EUR. COMM'N (May 2, 2017), https://ec.europa.eu/digital-single-market/en/news/final-results-european-data-market-study-measuring-size-and-trends-eu-data-economy. Such figures should be read to include both personal data and non-personal data, with personal data being important for services such as online advertising. As an example, close to $170 billion was spent worldwide on digital advertising in 2015 and this figure is expected to reach $330 billion by 2021. Google generates about $80 billion from digital advertising; Facebook, $27 billion. *See* Statista Research Department, *U.S. Digital Advertising Industry - Statistics & Facts*, STATISTA (Sep. 18, 2017), https://www.statista.com/topics/1176/online-advertising/.

34. "The European Union and the United States have the largest bilateral trade and investment relationship and enjoy the most integrated economic relationship in the world." *See Trade: Policy: Countries and Regions: United States*, EUR. COMM'N, https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (last visited on Aug. 22, 2019).

35. *See* Paul M. Schwartz & Karl-Niklaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 117 (2017) ("According to one estimate, the EU-U.S. economic relationship involves $260 billion in annual digital services trade. Cross-border information flows represent the fastest growing component of trade in both the EU and the United States") (citation omitted).

36. *See* Graham Greenleaf, *Countries with Data Privacy Laws—by Year 1973–2019* (May 10, 2019), https://ssrn.com/abstract=3386510 (showing countries and their respective laws concerning data privacy).

37. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 1096 (5th ed. 2015) [hereinafter INFORMATION PRIVACY LAW] ("Outside of Europe, other countries from around the world are moving toward adopting comprehensive privacy legislation on the European model.").

38. *See* Graham Greenleaf, *Global Data Privacy Laws 2019: New Eras for International Standards*, 157 PRIVACY L. & BUS. INT'L REP. 19–20 (2019), https://ssrn.com/abstract=3384012 ("the EU's GDPR has established a new 'global benchmark' for data privacy protection, to which non-EU countries are already aspiring to align their laws in very varying degrees.").

its model or aligned to fit it, serves the purposes of this study rather well, even if it is not perfect.

The study is structured as follows: in Part I the common principles at the heart of data privacy laws are exposed, as well as the subsequent divergence of privacy law and the consequences of such divergence, thus setting out the historical environment; then, in Part II obstacles to data privacy harmonization, which arise as a result of policy, political action, and the law—are discussed; next, in Part III, hopes for harmonization—whether through practice or law—despite the obstacles, are evaluated in the context of political and other realities; and finally, conclusory observations are drawn.

I. THE HISTORICAL CONTEXT: DATA PRIVACY LAW—FROM COMMON PRINCIPLES TO DIVERGENCE

Where today divergence is seen in data privacy law, originally there was convergence. In part this convergence arose from common principles at the heart of the law.[39] These are discussed in Section A, prior to investigating the eventual divergence in the law on one side and the other of the Atlantic (Section B) and its consequences (Section C).

A. Origins: Common Principles

Certain common principles underlay the data privacy laws of the United States and the European Union today, which originally were discussed in what has been described as "significant EU-U.S. policymaking interplay."[40] These principles first manifested themselves in the U.S. fair information practice principles and in early EU member state data privacy law, before taking an international turn in the Organisation for Economic Co-operation and Development (OECD) Guiding Principles, and then finding echo in the Council of Europe Convention 108, which has recently been modernized.[41] These common principles reflected an original transatlantic convergence in data privacy.[42] For comparison purposes, the Annex summarizes the principles in these various instruments and in the GDPR.

---

39. *See, e.g.*, Priscilla M. Regan, *Personal Information Policies in the United States and Britain: The Dilemma of Implementation Consideration*, 4(1) J. PUB. POL'Y 19, 20 (1984) (commenting, in an article that mainly focuses on data protection when data is collected by public bureaucracies, that "agreement quickly emerged in all countries that certain 'principles of fair information use' were necessary to protect an individual's privacy. Specific proposals were similar across countries, placing restrictions on bureaucratic collection, use and disclosure of information, as well as giving individuals rights over bureaucratic information practices.").

40. *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1970 (2013) ("First, there has long been a significant EU-U.S. policymaking interplay, which in this period included discussions of the policy instruments of FIP's and the development of the nonbinding OECD Guidelines.").

41. Council of Europe: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 10, 1985, ETS No. 108 (1985).

42. *See* Schwartz, *supra* note 40, at 1969 ("By the end of this period, there was a consensus that information privacy statute were to be constructed around Fair Information Practices (FIPs). This approach, shared in the United States and Western Europe alike, defines core obligations for organizations, whether in the public or private sector, that process personal information.").

1. Fair Information Practice Principles

The U.S. Department of Health, Education and Welfare (HEW) created a Secretary's Advisory Committee on Automated Personal Data Systems in 1972, in order to analyze the harmful consequences that might result from such systems.[43] The Committee investigated what is considered the first European data protection act—that of the German federal state of Hesse, which dates from 1970.[44] In addition, the Swedish Data Law of 1973[45] was examined. In 1973, the Committee produced a report, referred to as the "HEW Report,"[46] famous for setting out the fundamental principles used as the basis for the "Fair Information Practice Principles" (FIPPs).[47]

These FIPPs included principles about allowing individuals to know what information was being collected about them, its use, and giving a right to correct information when necessary. Individuals were to be given various rights.[48] Gloria González Fuster summarizes the FIPPs as follows:

> (1) no personal-data record-keeping system can be secret; (2) there must always be a way for individuals to find out what information about them is in the record and how it is used; (3) there must always be a way for individuals to prevent information obtained for one purpose from being used or made available for other purposes without their consent; (4) there must always be a way for individuals to correct or amend a record of identifiable information about them, and (5) any organisation creating, maintaining, using or disseminating records of identifiable personal data must assure the reliability of the data for their intended use, and must take reasonable precaution to prevent any misuse.[49]

Roughly speaking, the FIPPs summarized above correspond to what might be referred to today as principles of transparency (points 1 and 2), purpose specification (points 2 and 3), use limitation (point 3), data quality (points 4 and 5), and data security (also point 5), in addition to data subject rights. The FIPPs—influenced by the law of EU member states—in their turn helped shape early U.S. privacy legislation and on the international level, contributed to the

---

43. *See* GLORIA GONZÁLEZ FUSTER, THE EMERGENCE OF PERSONAL DATA PROTECTION AS A FUNDAMENTAL RIGHT OF THE EU 33 (2014) (detailing EU treatment of personal data protection).

44. *See id*.; *see also* Schwartz, *supra* note 40, at 1969 (providing a short history of EU data protection law and stating that EU data protection history began with a state-level law, when "the Hessian Parliament enacted the world's first comprehensive information privacy statute" in October 1970); *and* J. Lee Riccardi, *The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?*, 6 B.C. INT'L & COMP. L. REV. 243, 247 n.29 (also indicating that a German state-level law was enacted by Rhein-Pfalz a little over three years later, in January 1974).

45. *See* FUSTER, *supra* note 43; *see also* Schwartz, *supra* note 40; *and* Riccardi, *supra* note 44.

46. U.S. DEP'T OF HEALTH, EDUCATION & WELFARE, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records Computers and the Rights of Citizens (July 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf (Annex B to this Report: " 'Computers and Privacy': The Reaction in Other Countries," at 167–73, also details early data privacy legislation of EU member states).

47. WILLIAM MCGEVERAN, PRIVACY AND DATA PROTECTION LAW 619 (2016). FIPPs are also commonly referred to as "FIPs," although this study will retain the term "FIPPs."

48. *See* FUSTER, *supra* note 43, at 34–35.

49. *Id*. at 34 n. 86.

fashioning of privacy guidelines and a convention.[50] A consensus approach developed between the United States and Western Europe whereby data privacy laws were to be designed around the FIPPs.[51]

2. Organisation for Economic Co-operation and Development (OECD)

The Organisation for Economic Co-operation and Development (OECD) is an organization based in Paris that has as part of its mission "to shape policies that foster prosperity, equality, opportunity and well-being for all."[52] Today, its members number thirty-six, including, "many of the world's most advanced countries but also emerging countries . . . ."[53] On September 23, 1980, the OECD adopted what are commonly referred to as "the OECD Guidelines" in an effort to assist the harmonization of national legislation on privacy and data flows, in light of new technological developments that allowed the transmission of data internationally.[54] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data set out eight principles,[55] six of which resemble those of FIPPs. The OECD Guidelines, "represent an early and influential version of the FIPPs."[56] These go beyond the FIPPs and include an accountability principle, "enshrined in both E.U. data protection law and U.S. privacy law."[57] This accountability principle was also the subject of a new Article 15, requiring data controllers to implement a risk-based privacy management program, added to the OECD Guidelines in a 2013

50. *See* Schwartz, *supra* note 40, at 1969 ("By the end of this period, there was a consensus that information privacy statutes were to be constructed around Fair Information Practices (FIPs). This approach, shared in the United States and Western Europe alike, defines core obligations for organizations, whether in the public or private sector, that process personal information. The U.S. government and American privacy experts played an important part in this early global privacy debate. For example, a white paper from an advisory committee to the Secretary for Health, Education, and Welfare in the United States contained an influential early formulation of FIPs.").

51. *Id*.

52. *About the OECD*, OECD (last visited on Aug. 20, 2019), http://www.oecd.org/about/.

53. Today, OECD members include twenty-three of the twenty-eight EU member states (all *except* Bulgaria, Croatia, Cyprus, Malta, and Romania), three of the four the European Free Trade Association (EFTA) member states (Iceland, Norway, and Switzerland—all *except* Liechtenstein), Australia, Canada, Chile, Israel, Japan, Korea, Mexico, New Zealand, Turkey, and the United States. *Where: Global Reach*, OECD (last visited on Aug. 20, 2019) http://www.oecd.org/about/membersandpartners/.

54. *See* W. GREGORY VOSS & KATHERINE WOODCOCK, NAVIGATING EU PRIVACY AND DATA PROTECTION LAWS 3 (2015) (discussing the guidelines that were adopted to protect consumer privacy against increasing technological advances).

55. *The OECD Privacy Framework*, OECD, 14–15 (2013) [hereinafter OECD Guidelines], http://www.oecd.org/sti/ieconomy/oecd_ privacy_framework.pdf.

56. *See* Ira S. Rubinstein, *The Future of Self-Regulation Is Co-Regulation*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 509, 517 (Evan Selinger et al., eds., 2018) (citation omitted) (discussing the emergence of accountability as an important concept in privacy law and how the OECD incorporated it into their guidelines).

57. *Id*. at 510. The original accountability principle provided that, "A data controller should be accountable for complying with measures which give effect to the principles stated above." OECD Guidelines, *supra* note 55, at Annex, art. 14.

modernization.[58] The other principles include collection limitation,[59] data quality,[60] purpose specification,[61] use limitation,[62] security safeguards,[63] openness,[64] and individual participation.[65] Thus, the influential OECD Guidelines, which are what they are called—guidelines, and not a binding legal instrument—derive directly from the U.S. FIPPs and served to influence both U.S. and EU privacy law. Furthermore, they have influenced the drafting of the privacy framework of the Asia-Pacific Economic Cooperation (APEC), and the modernization version of the OECD Guidelines influenced APEC's updated framework in 2015, with, "due consideration for the different legal features and context of the APEC region."[66] However, another instrument—a binding international convention—would follow the original OECD Guidelines shortly after their publication.

---

58. *See* Rubinstein, *supra* note 56. The new Article 15 provides that data controllers should implement a privacy management program giving effect to the OECD Guidelines for personal data under their control and be prepared to demonstrate such program to relevant privacy authorities. Furthermore, controllers should provide data breach notifications when appropriate. OECD Guidelines, *supra* note 55, at art. 15.

59. The collection limitation principle provides that, "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." OECD Guidelines, *supra* note 55, at Annex, art. 7.

60. The data quality principle provides that, "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." *Id*. at art. 8. This resembles the data quality principle of the FIPPs.

61. The purpose specification principle provides that, "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." *Id*. at art. 9. This resembles the purpose specification principle of the FIPPs.

62. The use limitation principle provides that, in order to disclose, make available or use personal data for a different purpose, this must be done with the data subject's consent or by the authority of law. *Id.* at art. 10. This resembles the purpose specification principle of the FIPPs.

63. The security safeguards principle provides that, "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data." *Id*. at art. 11. This resembles the security safeguards principle of the FIPPs.

64. The openness principle provides that, "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." *Id*. at art. 12. This resembles the transparency principle of the FIPPs.

65. The individual participation principle provides to obtain information from the data controller on information collected relating to them, have that data communicated to them, to "challenge data relating to them" and, if successful, have such data "erased, rectified, completed or amended." *Id.* art. at 13. This resembles the rights of the data subject of the FIPPs.

66. *APEC Privacy Framework (2015)*, APEC (Aug. 2017), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015). This Framework is a "set of principles and implementation guidelines" and "set in motion the process of creating the APEC Cross-Border Privacy Rules system," or "CBPR System," which is described as analogous to the Privacy Shield, although "Unlike the GDPR, which is a directly applicable regulation, the CBPR system does not displace or change a country's domestic laws and regulations. Where there are no applicable domestic privacy protection requirements in a country, the CBPR system is intended to provide a minimum level of protection." *See* Alex Wall, *GDPR Matchup: The APEC Privacy Framework and Cross-Border Privacy Rules*, IAPP (May 31, 2017), https://iapp.org/news/a/gdpr-matchup-the-apec-privacy-framework-and-cross-border-privacy-rules/ (comparing different privacy frameworks from a global perspective). On the APEC CBPR system, Graham Greenleaf comments:

> after six years of operation, APEC CBPRs only involves a tiny number of US and Japanese companies. CBPRs is therefore of negligible practical significance as yet. The European Commission states in its Decision concerning Japan's adequacy assessment that certification of a company as APEC CBPRs compliant cannot be the basis for any onward transfer of EU-origin personal data from a country that is held to be GDPR-adequate. This will further diminish the business case for CBPRs.

Greenleaf, *supra* note 36, at 3 (citations omitted).

3. Convention 108

The Council of Europe, which describes itself as, "the continent's leading human rights organisation" with currently forty-seven members, including all EU member states,[67] in 1981 adopted the, "first legally binding international instrument in the field of data protection" which are built around the FIPPs[68]—Convention 108.[69] It is open for accession to countries from around the world, not just those in the Council of Europe.[70] It has a total of fifty-five accessions including (outside of the Council of Europe) Argentina,[71] Cabo Verde, Mauritius, Mexico, Morocco,[72] Senegal, Tunisia, and Uruguay. In addition, one other non-Council of Europe country has been invited to accede to the treaty but has not yet done so: Burkina Faso.[73] Professor Graham Greenleaf contends that:

> The steady expansion of Convention 108 beyond Europe is slowly making it apparent that it is the only viable global data privacy treaty, reinforced by its endorsement by both the EU's institutions and GDPR, and by the UN [Special Rapporteur on the Right to Privacy]. Progress toward the African Union's own treaty coming into force is gaining momentum but far from complete. APEC's CBPRs, despite ostensible participation, remains of negligible practical significance.[74]

This study will revert later to that EU endorsement in Part III.C.

Convention 108 applies both to data processing in the private and public sectors and protects data subjects against data processing abuses.[75] It is also

67. *Who We Are*, COUNCIL OF EUROPE, https://www.coe.int/en/web/about-us (last visited on Aug. 20, 2019) (discussing in addition to the EU member states (including the United Kingdom), the Council of Europe includes non-EU member states from EFTA (Iceland, Liechtenstein, Norway, and Switzerland), from the Balkan peninsula (Albania, Bosnia and Herzegovina, Montenegro, Serbia, and the Former Yugoslav Republic of Macedonia), from the former Soviet Union (Armenia, Azerbaijan, Georgia, Republic of Moldova, Russian Federation, and Ukraine), Western European principalities (Andorra, Monaco, and San Marino), and Turkey). *See Our Member States*, COUNCIL OF EUROPE, https://www.coe.int/en/web/about-us/our-member-states (last visited on Aug. 20, 2019) (showing a list of member states).

68. *See* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND 21 (2015) (discussing the importance of the FIP framework in developing guidelines for privacy protection).

69. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S No. 108, http://www.conventions.coe.int/Treaty/en/Treaties/Html/108.htm [hereinafter Convention 108].

70. DAVID WRIGHT, *Enforcing Privacy*, *in* ENFORCING PRIVACY 13, 33 (David Wright & Paul De Hert, eds., 2016).

71. Argentina ratified the Convention, on Feb. 25, 2019. In doing so, it became the third Latin American nation to accede to the Convention. *See* Press Release, Council of Europe, Argentina, 54th Party to Convention 108 (Feb. 28, 2019), https://www.coe.int/en/web/data-protection/-/argentina-54th-party-to-convention-108.

72. Morocco ratified the Convention most recently, however, on May 28, 2019. It became the sixth African nation to accede to the Convention and the 55th State party to the Convention. *See* Press Release, Council of Europe, Welcome to Morocco, 55th State Party to Convention 108 (May 28, 2019), https://www.coe.int/en/ web/data-protection/-/welcome-to-morocco-55th-state-party-to-convention-108-.

73. *Chart of signatures and ratifications of Treaty 108*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=zmoosUiP (last visited on Aug. 20, 2019); *see Non-members States of the Council of Europe: Five years validity of an invitation to sign and ratify or to accede to the Council of Europe's treaties*, COUNCIL OF EUROPE, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cac22 (last visited on Aug. 20, 2019) (indicating that the validity period for the invitation to Burkina Faso ends on Mar. 24, 2022).

74. Greenleaf, *supra* note 36, at 3.

75. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS & COUNCIL OF EUROPE, HANDBOOK ON EUROPEAN DATA PROTECTION LAW 24 (May 16, 2019).

meant to regulate cross-border personal data flows.[76] Furthermore, processing of sensitive data is generally prohibited, and data subjects should have various rights such as the right to information about processing of his or her data, and the right to rectification of such data.[77] Convention 108 is binding on the states that have ratified it.[78] Recently, Convention 108 has undergone a modernization, with an eye on ensuring its compatibility with EU legislation.[79] However, once again the impact of an early U.S. creation—the FIPPs—on EU data protection law may be seen, through an international convention adopted by all EU member states.

There are many elements in Convention 108 that relate to those of the FIPPs: the requirement that data be adequate, relevant and not excessive,[80] and that they be accurate and kept up-to-date,[81] related to data quality; purpose specification;[82] use limitation;[83] data security;[84] transparency of processing;[85] and rights of the data subject,[86] likewise relate to similar principles in the FIPPs. In addition, Convention 108 contains provisions on additional obligations[87] (similar to accountability in the OECD Guidelines) and legitimacy of data processing[88] (similar to collection limitation in the OECD Guidelines). The Annex summarizes the various principles contained in the instruments discussed above and in the GDPR, and thereby evidences the initial convergence of data privacy on both sides of the Atlantic and its continuance and development in the European Union.

B. What Happened? Divergence Settles In

Out of a common footing—the FIPPs—divergence of U.S. and EU data privacy law later appeared. This divergence manifested itself in the development of sectoral laws and self-regulation in the United States (Section 1), while omnibus data privacy legislation arose in the European Union (Section 2). Furthermore, certain other important differences between the ways the two systems handle data privacy law may be highlighted (Section 3).

---

76. *Id*.
77. *Id*. at 25.
78. *Id*.
79. *Id*. at 26–27.
80. Convention 108, *supra* note 69, at art. 5(4)(c) (requiring that personal data to be processed be "adequate, relevant and not excessive in relation to the purposes for which they are processed").
81. *Id*. at art. 5(4)(d) (requiring that personal data to be processed be "accurate and, where necessary, kept up to date").
82. *Id*. at art. 5(4)(b) (requiring that personal data to be processed be "collected for explicit, specified and legitimate purposes").
83. *Id*. at art. 5(4)(b) (requiring that personal data to be processed be "processed in a way incompatible with those purposes"; although an exception like that of GDPR art. 5(1)(d) applies).
84. *Id*. at art. 7(1) (requiring that "Each Party shall provide that the controller, and, where applicable the processor, takes appropriate security measures against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure of personal data.").
85. *Id*. at art. 8.
86. *Id*. at art. 9.
87. *Id*. at art. 10.
88. *Id*.

1. Development of Sectoral Laws and Self-Regulation in the United States

Where the FIPPs, as incorporated in the OECD Guidelines and Convention 108, had the vocation of applying globally to data privacy, the United States turned to the development of more limited sectoral laws instead.[89] An early sectoral data privacy law in the United States had already been adopted shortly before the HEW Report that established the FIPPs. The Fair Credit Reporting Act of 1970 (FCRA),[90] was adopted to protect individuals from the misuse of their personal information by Credit Reporting Agencies. The FCRA contained a form of FIPPs[91] established before the HEW Report. Following the FCRA, there also was the enactment of the Family Educational Rights and Privacy Act (FERPA)[92] in 1974, covering the access and disclosure of student educational records, not typically considered the domain of business law.

After the FCRA, the next major piece of federal privacy legislation to be adopted by the United States in business law was the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding healthcare data.[93] Then there was the Children's Online Privacy Protection Act of 1998[94] (COPPA) that dealt with children's information. That was followed by the Gramm—Leach—Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999,[95] in financial information. Each of these statutes is aimed at a specific sector of the population or of a limited economic sector.

However, Professor Paul Schwartz notes that some of what he calls "FIPs" (corresponding to the FIPPs) are not found in the U.S. data privacy regime, only one of which this study has included in the Annex (point (4), which is referred to (in the case of the OECD Guidelines) as legitimacy of data processing):

> (4) a processing of personal data made only pursuant to a legal basis; (5) regulatory oversight by an independent data protection authority; (6) enforcement mechanisms, including restrictions on data exports to countries that lack sufficient privacy protections; (7) limits on automated decision-making; and (8) additional protection for sensitive data.[96]

89. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 251 (2011) (discussing the fragmented nature of US privacy regulation and its lack of robust FIPPs).

90. Fair Credit Reporting Act, Publ. L. No. 91–507, 84 Stat. 1127 (codified at 15 U.S.C. §§ 1681-1681x (2018).

91. *See* Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. L. & POL'Y 728 (2007) (commenting that the FCRA, as well as the Privacy Act of 1974, "embraced a full set of FIPPS to protect personal information").

92. U.S.C. § 1232(g) (2018).

93. Health Information and Portability Accountability Act of 1996, Publ. L. No. 104-191, 110 Stat. 1936 (codified at 29 U.S.C. §1001(2016)).

94. Children's Online Privacy Protection Act of 1998, Publ. L. No. 105-277 tit. XIII, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501-6506 (2016)).

95. Gramm-Leach-Bliley Act (Financial Modernization Act of 1999), Publ. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. § 6801(2016)).

96. Schwartz also describes the greater emphasis of EU data privacy legislation, when compared to U.S. legislation, on principles of data quality (including data minimization), transparency (notice), and rights of data subjects (specifically, to access and correct their personal data). *See* Schwartz, *supra* note 40, at 1976. This study deals with Schwartz's points (5) and the enforcement mechanisms part of point (6) *infra* Section 3. The

Furthermore, as Professor Paul Ohm commented in 2015, even where U.S. sectoral laws such as HIPAA, FERPA,[97] and GLBA exist, they are narrower than EU legislation, as they are, "limited to particular actors in particular sectors."[98]

Also, the problem remains that there is an absence of any general data privacy law framework[99] against which the sectoral laws may add specificity,[100] much like specific terms and conditions of a contract provided without the general terms and conditions used to handle issues or cases not covered by the specific terms. In this way, the United States is an outlier,[101] avoiding international harmonization,[102] to the extent it exists.

Outside of the few instances when sectoral laws have been developed, often "isolated and very narrow statutes," adopted on a reactive basis following the disclosure of "particularly scandalous practices," there is no full set of standards.[103] This is the case for most of the areas in which the U.S. tech companies of Silicon Valley are involved.[104] Self-regulation is looked to for protection of privacy, even though such practice led to an absence of FIPPs in U.S. society.[105] Such self-regulation is based on resolution of privacy values by the marketplace, which is not the typical way to deal with political rights in a

---

restrictions on data exports part of point (6) is mentioned, from an EU perspective, *infra* Section C. Point (7) is mentioned briefly in connection with rights of data subjects under the GDPR *infra* Section 2. For a discussion of the difference between the treatment of sensitive data in the European Union and the United States (Schwartz's point (8)), not discussed in this study other than in connection with Convention 108, *see supra* Section A.2; *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, 422–425 (2013) (discussing what constitutes sensitive data, according to the EU).

97. Family Educational Rights and Privacy Act of 1974, Pub. L. No. 93-380, Tit. V, § 513, 88 Stat. 57 (1974) (codified at 20 U.S.C. § 1232g (2018), 34 C.F.R. Part 99) (FERPA)). This statute, which deals with students' personal information, is outside the scope of traditional business law areas, as it only covers educational agencies and institutions receiving funding under a program administered by the U.S. Department of Education.

98. Ohm, *supra* note 28, at 1190 (considering the tie made by these U.S. statutes between risk of harm and the type of entity holding information probably to be an obsolete view of information. For example, cloud service providers, even though not covered by HIPAA, may hold sensitive health information; *id*., at 1190–91 (citation omitted)).

99. *See, e.g.*, Greenleaf, *supra* note 23, at 549 (explaining that "the USA has no comprehensive data privacy laws of its own").

100. *See, e.g.*, Schwartz, *supra* note 40, at 1974 (describing sectoral laws as "a backup used to increase the specificity of regulatory norms stemming from the initial statutory framework").

101. *See id*. (describing the United States as "the great exception regarding the international preference for omnibus legislation.").

102. *See, e.g.*, GREENLEAF, *supra* note 23, at 7 (stating that data privacy laws are "becoming ubiquitous among the world's countries" and that the main influence on such laws outside of Europe "will be shown to be 'European standards'"). In his book, Greenleaf considers that a country has a "data privacy law" only "if it has a national law which provides, in relation to most aspects of the operation of the private sector, or its national public sector, or both, a set of basic data privacy principles , to a standard at least including most of the OECD Guidelines or [Convention 108], plus some methods of statutorily mandated enforcement (i.e. not only self-regulation)." *Id*., at 6. For our purposes, only legislation affecting the private sector is of interest.

103. Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 664–665 (2014).

104. *See id.* (referring to U.S. data privacy law as offering "limited constraints for American Internet entrepreneurs," with quite narrow statutory protections).

105. *See* Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce Symposium – The Legal and Policy Framework for Global Electronic Commerce: A Progress Report*, 14 BERKELEY TECH. L.J. 771, 774 (1999) (referring to studies that evidence such lack of FIPPs, while government agency task forces "resorted to the mantra that business should be given more time to self-regulate"). Reidenberg describes the self-regulation theory of the last two decades of the twentieth century as "pure sophistry." *Id.* at 776.

democracy, and the working of the market may be hampered by its lack of transparency in the area of personal data.[106] Nonetheless, self-regulation does fit with a *laissez-faire* policy, which is the predominant position in the United States.[107] Professor Anupam Chander has described the end result of this as "while Facebook's and Google's innovations have often drawn public outcries, they seldom draw successful lawsuits or government enforcement actions."[108]

2. Omnibus Data Privacy Legislation in the European Union: The 1995 Directive and the GDPR

As the United States was adopting sectoral data privacy laws, the European Union turned to omnibus legislation,[109] instead. European Union Directive 95/46/EC (1995 Directive)[110] required EU member states to implement (or transpose) into their national law its requirements, thereby creating "strong incentives for omnibus legislation within the EU," which had been the path chosen for previous EU member state legislation, as well.[111]

The 1995 Directive incorporated forms of the FIPPs. It contains a purpose limitation (or finality) principle, combining the concepts of purpose specification and use limitation (or compatible use).[112] It includes the data quality principle, divided up into a requirement of accuracy,[113] and also what we might today refer to as data minimization (or the proportionality principle).[114] The 1995 Directive has a storage limitation provision,[115] a notice (or

106. *See id.* at 775 (positing that "for personal information, the natural tendency of the marketplace is to obscure its treatment," and stating that this is "a classic case of market failure").

107. *See infra* Part II.A.

108. Chander, *supra* note 103, at 668.

109. INFORMATION PRIVACY LAW, *supra* note 37, at 1096. Omnibus data privacy legislation in Europe has been described as follows: "one statute typically regulates the processing of personal information in public and private sectors alike. In the absence of more specific legislation, the general information privacy law in Europe sets the initial terms for the processing, storage, and transfer of personal information. The omnibus law is often accompanied, moreover, by more specific privacy laws."

110. 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 1995 Directive].

111. *See* Schwartz, *supra* note 40, at 1974 (explaining that, "'Omnibus' privacy laws establish regulatory standards with a broad scope" (citation omitted)).

112. *See* 1995 Directive, *supra* note 110, art. 6(1)(b) (requiring that personal data be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes," but allowing further processing (subject to member states providing safeguards) for "historical, statistical or scientific purposes. . . .").

113. *Id*. at art. 6(1)(d) (requiring that personal data be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or complete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified . . . .").

114. *Id*. at art. 6(1)(c) (requiring that personal data be "adequate, relevant and not excessive in relation to the purposes for which they were collected or for which they are further processed . . . .").

115. *Id*. at art. 6(1)(e) (requiring that personal data be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed" with the possibility for member states to set safeguard standards for longer storage for historical, statistical or scientific use).

information) requirement (transparency principle),[116] rights of data subjects,[117] and a security of processing requirement (security principle),[118] as well. Furthermore, processing had to be fair and lawful,[119] with the data controller being responsible for ensuring most data protection obligations were met (accountability).[120]

With the adoption of the GDPR in 2016, the European Union continued to develop its data protection law based on the FIPPs, in a form applicable in all business sectors—true omnibus data privacy legislation. Among the GDPR's data protection principles may be found several elements which evolved from the FIPPs: in data quality, accuracy[121] and data minimization;[122] purpose limitation,[123] which subsumes the FIPPs' elements of purpose specification and use limitation, and a related concept of storage limitation;[124] integrity and confidentiality,[125] which is a development of the security safeguards under the FIPPs; transparency;[126] and significantly expanded rights of the data subject, which now include a right of access, and rights to rectification, to erasure ("right to be forgotten"), to restriction of processing, to data portability, to object, and not to be subject to automated decision-making or profiling, subject to certain exceptions.[127] In addition, other principles similar to those of the OECD

116. *Id*. at arts. 10–11 (requiring certain information to be provided to the data subject, depending on whether or not the collection of the personal data was directly from the data subject (*id.* art. 10), or indirectly, instead (*id*. art. 11)).

117. *Id*. at arts. 12, 14, and 15 (providing data subjects with a right to access their data and, as appropriate, require that it be rectified, erased or blocked if not in compliance with the 1995 Directive (e.g., if incomplete or inaccurate) (*id*. art. 12); with a right to object to processing (*id*. art. 14); and a right, subject to a couple of exceptions, not to be subject to automated individual decisions having legal effects (*id*. art. 15).

118. *Id*. at art. 17.

119. *Id*. at art. 6(1)(a). This requirement should be read in conjunction with the requirement that data processing had to have a legitimate basis under Article 7.

120. *See, e.g., id*. at art. 6(2) (making it the controller's responsibility to ensure that data quality, proportionality, and fair and lawful processing requirements are met); *see also id*. at arts. 10 and 11(1) (establishing transparency as a responsibility of the controller), and at art. 17(1) and (2) (making the controller responsible for security, even when a processor carries out processing on its behalf).

121. GDPR, *supra* note 16, at art. 5(1)(d) (requiring personal data to be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.").

122. *Id*. at art. 5(1)(c) (requiring personal data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.").

123. *Id*. at art. 5(1)(b) (requiring personal data to be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" and providing an exception for further processing "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.").

124. *Id*. at art. 5(1)(e) (requiring personal data to be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" with a conditional exception for archiving purposes).

125. *Id*. at art. 5(1)(f) (requiring personal data to be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.").

126. *Id*. at art. 5(1)(a) (requiring personal data to be processed "in a transparent manner in relation to the data subject"). This requirement should be read together with requirements of information to be provided to the data subject regarding data collection contained in *id*. arts. 13–14).

127. *Id*. at arts. 15–22 (these rights should be read in conjunction with *id*. art. 12 requiring information to be provided to the data subject about the exercise of his or her rights).

Guidelines and Convention 108 are also included: accountability[128] and lawfulness and fairness of processing.[129]

3. Certain Differences between U.S. and EU Handling of Data Privacy Law

In addition to the major difference between sectoral data privacy legislation (in the United States) and omnibus legislation (in the European Union), and the well-developed rights of the data subject under European Union law, as mentioned in Section 2, which do not generally exist in the United States, there are certain differences in how data privacy law is handled on the two sides of the Atlantic. This study mentions just a few of these below.

The European Union has chosen to adopt a broad definition of personal data, which may include more indirectly-identifying data than the U.S. term "personally identifiable data" or "PII."[130] As an example, in the European Union internet protocol (IP) addresses may be considered as "personal data" in certain circumstances,[131] whereas divergence in court decisions exists on this point under applicable U.S. legislation.[132] Under the GDPR, once personal data exists, its processing (a very broad term) requires a legitimate basis, of which consent is the prime example.[133] If consent is the basis for collection of data, not only must there be transparency about the processing, including the purpose specification (and use limitation) set out by the FIPPs, but consent must be demonstrable, specific, and subject to withdrawal.[134] Personal data collected may not be exported to a country outside of the European Union unless such country provides an adequate level of data protection,[135] contrasting with the United States' lack of specific rules for such data transfers outside of its borders.[136]

---

128. *Id*. at art. 5(2) (the "controller shall be responsible for, and able to demonstrate compliance with" the GDPR data protection principles). This is related to accountability under the OECD Guidelines, and additional obligations under Convention 108.

129. *Id*. at art. 5(1)(a) (requiring personal data to be processed "lawfully, fairly"). This requirement should be read in conjunction with *id*. art. 6 (setting out the bases for lawfulness of processing) and, where the basis for processing is consent of the data subject, *id*. at art. 7 (establishing the conditions for consent) and, if applicable, *id*. at art. 8 (setting out conditions applicable to a child's consent). This category is similar to collection limitation under the OECD Guidelines and legitimacy of data processing under Convention 108.

130. *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and A New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1823 (2011) (explaining the differences in the personal data definitions between the EU and the U.S.).

131. *See e.g.*, Voss & Houser, *supra* note 24, at 318–320 (discussing the difference between PI and personal data).

132. *Id*. at 305.

133. *Id*. at 326. The other potential bases, which include the case when processing of the data is "necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract," are set out in GDPR, *supra* note 16, at art. 6(1).

134. GDPR, *supra* note 16, at art. 7. For a discussion of consent, *see* Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1 (2018), at ¶¶ [81]–[83] [hereinafter Houser & Voss] (comparing the GDPR's affirmative consent requirements to the U.S. opt-out model).

135. *See infra* Part I C (focusing on cross-border data transfer restrictions).

136. *See, e.g.*, Shawn Marie Boyne, *Data Protection in the United States*, 66 AM. J. COMP. L. 299, 341 (2018) ("Consistent with the U.S. national commitment to free and fair trade, the United States does not have many specific rules that govern the transfer of data outside of the country, beyond the "basic fair information principles for notice and prohibitions on deceptive or unfair business practices." (citation omitted)).

In the European Union, independent supervision of data processing is considered part of the checks and balances necessary for protection of data subjects under the fundamental right of data protection.[137] Each member state is required to have an independent administrative authority responsible for monitoring application of the GDPR "in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data" with the European Union (such as the CNIL in France) and referred to as a "supervisory authority."[138] Members of supervisory authorities are required to act "with complete independence,"[139] "remain free from external influence, whether direct and indirect," "neither seek nor take instructions from anybody,"[140] and appointed by means of a "transparent procedure."[141] Member state law establishes the "conditions governing the obligations of the member or members and staff of each supervisory authority, prohibitions on actions, occupations and benefits incompatible therewith during and after the term of office."[142] A duty of professional secrecy exists, both during and after employment, with respect to any confidential information "which has come to their knowledge in the course of the performance of their tasks or exercise of their powers."[143]

Among their powers (without being exhaustive), supervisory authorities may carry out investigations,[144] notify alleged infringements to controllers and processors,[145] issue warnings,[146] reprimands,[147] impose limitations and bans on processing[148] and administrative fines.[149] Importantly, these administrative fines may now be assessed up to a maximum of the greater of €20 million or four percent of annual global revenue (turnover) in the most serious cases.[150] Each of these powers is in connection with data privacy law—particularly, the GDPR and any specific member state provisions allowed by the GDPR, and contrasts with the situation in the United States, where privacy has been "enforced in limited sectors with no consistent regulatory oversight," even if based on the FIPPs similar to those in the European Union.[151]

137. *See* HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 75, at 19 (outlying procedures of independent supervision of data processing); *see also infra* Part II.C (discussing the right to data protection).

138. GDPR, *supra* note 16, at art. 51(1). Sometimes supervisory authorities are commonly referred to as "data protection agencies," "data protection authorities," or "DPAs."

139. *Id*. at art. 52(1).

140. *Id*. at art. 52(2).

141. *Id*. at art. 53(1). This procedure may involve an appointment by the member state's parliament, government, head of State, or by an "independent body entrusted with the appointment under Member State law."

142. *Id*. at art. 54(1)(f).

143. *Id*. at art. 54(2).

144. *Id*. at art. 58(1)(b).

145. *Id*. at art. 58(1)(d).

146. *Id*. at art. 58(2)(a).

147. *Id*. at art. 58(2)(b).

148. *Id*. at art. 58(2)(f).

149. *Id*. at art. 58(2)(i).

150. *Id*. at art. 83(5).

151. *See* BAMBERGER & MULLIGAN, *supra* note 68, at 22 (comparing certain data privacy law enforcement actions in the European Union and the United States); Houser & Voss, *supra* note 134, at 20–52 (discussing Facebook and Google privacy cases).

The United States has no *de jure* independent data privacy authority, in the same sense as the European Union.[152] The *de facto* data privacy authority—the Federal Trade Commission (FTC)[153]—suffers from many handicaps in its action.[154] The FTC was not charged with the enforcement of privacy but was given the role of fighting unfair and deceptive trade practices, which might include failure to comply with privacy policies when they are supplied by companies.[155] Furthermore, the FTC has limited jurisdiction and does not cover, for example, sectors such as transportation, insurance, banking, and telecommunications.[156] Added to this limited jurisdiction is the fact that the FTC cannot "engage in broad rulemaking for privacy," although under some statutes such as COPPA it may have some rulemaking power.[157] Moreover, whatever power the FTC has, it has not used to its full extent.[158]

FTC enforcement cases have mainly resulted in consent agreements,[159] while the effectiveness of such agreements, which are memorialized by the FTC in consent orders, have come under question and their oversight by the FTC have even been described as "box-checking exercises."[160] On November 27, 2018, the U.S. Senate Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security held a "Oversight of the Federal Trade Committee" hearing to report the FTC's priorities.[161] One journalist reported the proceedings as focusing in part on the FTC's "poor track record" for enforcement, and the potential lack of deterrent effect of its actions.[162]

---

152. Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U L. REV. 1, 21 (2019).

153. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014) ("Today, the FTC is viewed as the de facto federal data protection authority." (citations omitted)).

154. *See id.* at 605 ("Indeed, the FTC lacks the general authority to issue civil penalties and rarely fines companies for privacy-related violations under privacy-related statutes or rules that provide for civil penalties.").

155. 15 U.S.C. § 45(a)(2); *see* Houser & Voss, *supra* note 134, at 14 (explaining this power is derived from Section 5 of the FTC Act: "[t]he Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except . . . from using unfair methods of competition in or affecting commerce.").

156. *See* Robert Gellman & Pam Dixon, *Failures of Privacy Self-Regulation in the United States*, ENFORCING PRIVACY 53, 72 (David Wright & Paul De Hert, eds., 2016) ("[T]he Commission does not have authority over the entire US economy. In general, it has limited or no authority over privacy activities of federal state and local agencies, most non-profit organisations, and many commercial entities engaged in transportation, insurance, banking and telecommunications.").

157. *Id*. at 73.

158. *Id*. ("Self regulation provides the promises that the Commission can seek to enforce, but the Commission has not done so.").

159. Marc Groman, *The Critical Importance of the FTC Enforcement Record*, IAPP (Jan. 15, 2015), https://iapp.org/news/a/the-critical-importance-of-the-ftc-enforcement-record/ ("Since the late 1990s, the FTC has brought approximately 180 privacy and data security related enforcement actions, most of which have resulted in the publication of consent agreements with the defendants.").

160. *See* Joseph Jerome, *Can FTC Consent Orders Effectively Police Privacy?*, IAPP (Nov. 27, 2018), https://iapp.org/news/a/can-ftc-consent-orders-police-privacy/ ("But as the FTC's oversight of Facebook reaches its midpoint, there is growing evidence that these orders simply create box-checking exercises without protecting anyone's privacy.").

161. Press Release, FED. TRADE COMM'N, FTC Testifies Before Senate Commerce Subcommittee About the Agency's Work to Protect Consumers, Promote Competition, and Maximize Resources (November 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/11/ftc-testifies-senate-commerce-subcommittee-about-agencys-work.

162. Rhett Jones, *FTC Won't Even Tell the Senate If It's Going to Try to Squeeze a Trillion-Dollar Fine Out of Facebook*, GIZMODO (Nov. 27, 2018, 7:03 PM), https://gizmodo.com/ftc-wont-even-tell-the-senate-if-its-going-to-try-to-sq-1830688190) ("There were two major issues that came up again and again during the hearing:

Thus, what enforcement actions have been taken may not have been effective. An example of this may be the Facebook consent decree, which required Facebook to give clear notice and obtain express consent from consumers before sharing data beyond privacy settings,[163] which the advocacy group EPIC claimed Facebook did not do in the case of WhatsApp user data that was transferred to Facebook.[164] Furthermore, the FTC investigated whether the Cambridge Analytica incident was a violation of the consent decree,[165] and finally in July 2019, entered into a $5 billion settlement with Facebook regarding charges that it violated the 2012 consent decree,[166] seemingly indicating a failure of the consent decree enforcement measure, and serving as the exception that proves the rule. The case is exceptional, not only for the amount of the settlement, but also because based on the claim that Facebook: (i) deceived users to undermine their privacy preferences, in violation of the 2012 consent decree, and (ii) took insufficient measures with respect to apps violating Facebook policies.[167] Furthermore, it is exceptional because of the nature of the related Cambridge Analytica affair, one of the events highlighted in the introduction to this study.[168] However, critics have claimed that the settlement is ineffectual.[169]

Contrasting the failure of FTC action under consent decrees with continuing EU data protection agency follow-up on various data protection violation issues is an interesting exercise. Many cases have been taken against

---

the FTC's claim that it needs more resources and everyone's acknowledgment that the agency has a poor track record when it comes to enforcement. In his opening statement, Commissioner Rohit Chopra tied the two issues together, saying that too often the FTC is willing to accept a settlement in order to avoid a costly trial. "While big penalties made for good headlines, I question whether they truly deterred lawbreaking," Chopra said."); *see also Oversight of the Federal Trade Commission: Hearing before Subcomm. on Consumer Prot., Prod. Safety, Ins., and Data Sec.* (2018) (statement of U.S. Sen. Jerry Moran, chairman of the Subcomm. on Consumer Prot., Prod. Safety, Ins., and Data Sec.) (providing an archived webcast of the hearing).

163. Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; Houser & Voss, *supra* note 134, at 42.

164. *See* Houser & Voss, *supra* note 134, at 42. Note that the digital rights group, Electronic Privacy Information Center (EPIC), which is very critical of the FTC, calls for the United States to institute a proper DPA and comments on data security: "The Federal Trade Commission is fundamentally not a data security agency. The FTC only has authority to bring enforcement actions against unfair and deceptive practices in the marketplace, and it lacks the ability to create prospective rules for data security. The Consumer Financial Protection Bureau similarly lacks data protection authority and only has jurisdiction over financial institutions. Neither of these agencies possess the resources needed to address data security." *See The U.S. Urgently Needs a Data Protection Agency*, EPIC.ORG, https://epic.org/dpa/ (last visited on Aug. 23, 2019).

165. Houser & Voss, *supra* note 134, at 43.

166. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

167. *See id*. ("'Despite repeated promises to its billions of users worldwide that they could control how their personal information is shared, Facebook undermined consumers' choices,' said FTC Chairman Joe Simons.").

168. *See id.* ("Cambridge Analytica['s] . . . former Chief Executive Officer Alexander Nix, and Aleksandr Kogan, an app developer who worked with the company, alleg[ed] [Cambridge Analytica] used false and deceptive tactics to harvest personal information from millions of Facebook users.").

169. *See, e.g.*, Rob Price, *The US Government Says Ditching Its Controversial $5 Billion Settlement with Facebook Could Result in a 'Far Worse' Deal for Consumers*, BUS. INSIDER (Aug. 5, 2019, 8:04 PM), https://www.businessinsider.com/us-abandoning-facebook-ftc-settlement-could-result-worse-outcome-2019-8?IR=T ("The Electronic Privacy Information Center (EPIC), a privacy-focused non-profit organization, is one such critic. It filed a motion to intervene in the case, arguing the settlement "is not adequate, reasonable, or appropriate").

Google and Facebook in the European Union.[170] Recently, the French Data Protection Agency, the CNIL—just one of 28 such agencies in the European Union—imposed a $57 million fine on Google for data privacy violations,[171] more than twice the then-largest FTC fine to date[172] (although much less than the exceptional 2019 Facebook settlement). In addition, an example of the FTC's relatively lax attitude in the past was its failure for years to effectively enforce the 2000 Safe Harbor agreement between the European Union and the United States, which allowed for the export of personal data from the former to the latter, in cases where companies receiving the data had self-certified to the scheme, agreeing to principles to provide safeguards to the data and rights to data subjects.[173]

As elements of U.S. data privacy law may appear to be more consumer protection law than data privacy law[174] (this is even apparent in the choice of data privacy authority—the FTC instead of a true independent supervisory authority), it is logical that the focus of protection in the United States has been on the consumer and not the data subject. While the two may be one and the same, a data subject does not need to *consume*, in the any sense of the word (whether goods or services be for pay or free), to benefit from the GDPR's protections. The GDPR, like the 1995 Directive before it, protects the personal data of individuals even outside of the professional/consumer relationship.[175] For example, under the 1995 Directive, images of a data subject caught on video camera walking down the street were found to be protected as personal data under the 1995 Directive in a case involving a non-commercial setting where an

170. *See* Houser & Voss, *supra* note 134, at 20–35.

171. *See* Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://nyti.ms/2HxCDNw (noting that Google announced a few days later that it is appealing the CNIL's decision); David Meyer, *Google Appeals $57 Million Privacy Fine in Europe*, FORTUNE (Jan. 24, 2019), http://fortune.com/2019/01/24/google-appeals-eu-privacy-fine/.

172. *See* Tony Romm, *The FTC and Facebook are Negotiating a Record, Multibillion-Dollar Fine for the Company's Privacy Lapses*, WASH. POST (Feb. 14, 2019, 4:18 PM), https://www.washingtonpost.com/technology/2019/02/14/us-government-facebook-are-negotiating-record-multi-billion-dollar-fine-companys-privacy-lapses/ (reporting that the largest FTC fine to date on a tech giant for breaking an agreement with the government on safeguarding consumer data was a $22.5 million penalty paid by Google in 2012. EPIC Executive Director Marc Rotenberg commented that, "It is an open question at this moment in time whether the Federal Trade Commission is an effective privacy agency, and it is also an open question as to whether the FTC is willing to use its current authority to safeguard consumer privacy in the United States," while a large fine could offer reassurance in this regard.).

173. *See* W. Gregory Voss, *The Future of Transatlantic Data Flows: Privacy Shield or Bust?*, 19 J. INTERNET L. 1, 11 (May 2016) ("US authorities (the FTC) did not take proactive action to monitor compliance with the engagements of companies prior to 2009, and early enforcement action sanctioned merely misstatements as to companies' certifications being current (that is, having been renewed). Enforcement actions truly based on a review of compliance appear only to have commenced in 2011 (Google Buzz case), and really to have picked up in 2014 after EU review and investigation in late 2013 and 2014 following the Snowden NSA program revelations.").

174. *See* Schwartz & Peifer, *supra* note 35, at 119 (noting that in the absence of the fundamental rights held by EU data subjects, the "U.S. legal system favors its data processors over its privacy consumers."). Schwartz & Peifer refer to a difference between "rights talk" in the European Union, which protects "data subjects" and is part of a "constitutional task," and a "marketplace discourse" in the United States, focused on the protection of "privacy consumers," with data privacy law "based on the idea of consumers whose interests merit governmental protection in a marketplace marked by deception and unfairness."

175. *See id.* at 141 (emphasizing the strong continuity of the 1995 Directive in the GDPR).

individual set up the camera to ensure the security of his personal home.[176] In that case, no professional/consumer relationship existed.[177] This treatment, where protections that are available for data subjects are available regardless of status as a consumer or not, is fully consistent with the fundamental rights nature of data protection in the European Union, discussed in Part II.C *infra*. It would seem hard to reconcile the two attitudes, given that the differences in legal culture are substantial.

C. Consequences for Business: Safe Harbor and Privacy Shield; Certain Public Security and Justice Issues

The consequences for businesses of a lack of harmonization include having to set up compliance programs for differing legislation, and potentially suffering from restrictions on export of personal data from one country to another. In its introduction, this study mentioned the benefit of harmonization in allowing a company to comply with one set of rules.[178] Now it will focus on cross-border data transfer restrictions. In this context, this study also mentions public security and justice issues, which have had an impact on the perceived adequacy of U.S. data privacy protections.

In the 1995 Directive, a provision restricting the transfer of personal data to "third countries" (that is, outside the European Union), unless the third country "ensures an adequate level of protection" was included.[179] Adequacy of data protection was to be assessed by a review of several factors, the most germane for this study's purposes being "the country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."[180] Where a third country was found by the Commission not to ensure an adequate level of data protection, member states were to "take the measures necessary to prevent any transfer of data of the same type to the third country in question."[181]

As the United States did not receive an adequacy decision from the Commission, there was a threat that personal data transfers from the European Union to the United States would be halted.[182] The Commission negotiated with the U.S. Department of Commerce and created a Safe Harbor framework, whereby companies in the United States could self-certify adherence to the framework's principles, giving more or less equivalent rights to data subjects as

176. 2014 E.C.J. 2428.

177. 1995 Directive, *supra* note 110, art. 25(1).

178. *Reforming the U.S. Approach to Data Protection and Privacy*, CFR.ORG, https://www.cfr.org/report/reforming-us-approach-data-protection (last visited Sep. 17, 2019).

179. 1995 Directive, *supra* note 110, art. 25(1).

180. *Id*. art. 25(2).

181. *Id*. art. 25(4).

182. *See* Voss, *supra* note 16, at 230 ("In 1995, the European Union did not consider the United States to be a country that ensured an adequate protection level for personal data.").

those provided under the 1995 Directive, and continue to receive personal data from the European Union.[183]

After the September 11, 2001 terrorist attacks in the United States, Congress passed the Patriot Act and "instituted a host of other measures that dramatically increased the warrantless collection of personal information," which combined with other factors, created a political environment unfavorable to the adoption of omnibus data privacy legislation.[184] While certain measures were taken to provide surveillance powers in EU countries such as Germany and France,[185] these have generally been seen not to go as far as U.S. legislation.[186] During the period prior to 2015, the Safe Harbor remained unaffected by these developments, although, following the disclosure of the NSA's mass surveillance program, the Commission recommended changes to the Safe Harbor,[187] and an Austrian law student brought a lawsuit against Facebook that would lead to the invalidation of the Safe Harbor (then relied upon by Facebook for data transfers) in the ECJ.[188] In the ECJ case, *Schrems v. Data Protection Commissioner*, the fact that the U.S. authorities could access personal data of EU persons in connection with mass surveillance was at the heart of concerns in the ECJ's decision to invalidate.[189] In 2016, the Commission and the

183. *See id.* ("In 2000, the U.S. Department of Commerce ("DoC") and the European Commission negotiated the U.S.–EU Safe Harbor, which the European Commission then established under an "adequacy" decision in order to allow personal data transfers to U.S. companies that self-certified their compliance with the substance of EU data protection law.").

184. *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 113–114 (2019) (citing Peter Swire for the proposition that "[w]ith the attacks of September 11, 2001, everything changed. The new focus was overwhelmingly on security rather than privacy.").

185. *Id*. at 114; *see generally* Céline Castets-Renard, *Online Surveillance in the Fight Against Terrorism in France*, EU INTERNET L. REG. & ENF'T 385 (Tatiana-Eleni Synodinou et al., eds., 2017), https://ssrn.com/abstract=3391256 (explaining the surveillance regulations in France); *see also* W. Gregory Voss, *After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change*, 71 BUS. LAW. 281, 285–89 (2015) (noting the legislative reaction of France to the Charlie Hebdo terrorist attacks).

186. *See* Wanda Mastor, *The French Intelligence Act: "The French Surveillance State?" A Comparison with the USA Patriot Act and Freedom Act*, 23 EUR. PUB. L. 707, 709 (2017) ("The [2015 French Intelligence] Law may be criticized for the content, even for its omissions, but the claim that it is a French clone of the US PATRIOT Act must be vigorously—and scientifically—rejected.").

187. MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RESEARCH SERV., R44257, U.S. - EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD 5 (2016).

188. Voss, *supra* note 16, at 230–31.

189. 2016 E.C.J. 650. The ECJ in this case remarked that the Safe Harbor adequacy "decision thus enables interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States." *Id*. at 87. Furthermore, the Safe Harbor adequacy decision "does not contain any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with the fundamental rights of the persons whose data is transferred from the European Union to the United States, interference which the State entities of that country would be authorised to engage in when they pursue legitimate objectives, such as national security." *Id*. at 88. In addition, the Safe Harbor's dispute resolution mechanisms were for the use in "commercial" disputes with the companies involved, not when the dispute originated with such action of the U.S. authorities. *Id*. at 89. The ECJ considered that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life." *Id*. at 94. Finally, the ECJ noted that the Commission never stated in its decision that the United States, "in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments." *Id*. at 97. These concerns may be summarized as follows: Safe Harbor "enabled transfer of data of EU citizens to the United States, but failed to prevent surveillance of that data by U.S. sources to a sufficient extent as

Department of Commerce negotiated the Privacy Shield, which likewise involved a self-certification system, to replace the Safe Harbor.[190] That same year, the GDPR was adopted, continuing requirements for adequacy of data protection in order to allow for data exports to the United States.[191] In the process, the criteria for assessing adequacy have been modified, taking a more "respect for fundamental freedoms"[192] and "independent supervisory authorities"[193] turn.

However, challenges to the Privacy Shield, which also take into consideration access to personal data by U.S. authorities, are in the courts, and these pose risk for the basis for export of personal data from the European Union to the United States, and to alternative methods for such export (for example, standard contract clauses).[194] A far more comfortable position would exist if there was harmonization of the data privacy law of the United States with that of the European Union, based on the FIPPs, and including a true independent supervisory authority charged with ensuring and enforcing compliance with the U.S. law, in such a way that the United States could obtain an adequacy decision from the Commission based on U.S. legislation. However, obstacles to such harmonization exist,[195] and furthermore, there is no guarantee that such a decision could be obtained with current U.S. mass surveillance programs in place.[196]

---

required by the [1995] Directive." *See* Robert Hash, *Fundamental Differences in Privacy Laws Can Undermine Economic Ties and Multinational Corporate Plans: What Companies Can Do to Prepare for the Next Safe Harbor Moment*, 42 N.C. J. INT'L L. 1061, 1079 (2017).

190. Voss, *supra* note 16, at 231–32.

191. GDPR, *supra* note 16, at art. 45(1).

192. *Id*. art. 45(2)(a) (noting that criteria in this sense include: "the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country … which are complied with in that country …, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred.").

193. *Id*. art. 45(2)(b) (explaining that criteria here include: "the existence and effective functioning of one or more independent supervisory authorities in the third country …, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States."); *but see infra* Part B.3 (detailing the absence of an U.S. independent supervisory authority, as such concept is understood in the European Union).

194. *See* Kimberly A. Houser & W. Gregory Voss, *The European Commission on the Privacy Shield: All Bark and No Bite?*, U. ILL. J.L. TECH. & POL'Y: TIMELY TECH (Dec. 20, 2018), http://illinoisjltp.com/timelytech/the-european-commission-on-the-privacy-shield-all-bark-and-no-bite/ (discussing the U.S.'s tenuous commitment to the Privacy Shield mechanism and risks to the latter posed by the *Schrems II* case). *See* Jennifer Baker, *Groundhog Day for Privacy Shield Review*, CPO MAGAZINE (Sept. 24, 2019), https://www.cpomagazine.com/data-protection/groundhog-day-for-privacy-shield-review/ (discussing Privacy Shield's third annual review and NGO Access Now's call for the European Commission to strike down the arrangement, and mentioning the court challenge to the Privacy Shield by French digital rights group La Quadrature du Net and others). *See also* Catherine Stupp, *Companies Face Uncertainty Over Challenges to Trans-Atlantic Data Transfers*, WSJ (Sept. 23, 2019 11:18 am ET), https://www.wsj.com/articles/companies-face-uncertainty-over-challenges-to-trans-atlantic-data-transfers-11569013484 (discussing the challenges to the Privacy Shield and standard contractual clauses by Max Schrems and a privacy nonprofit before the ECJ).

195. *See Reforming the U.S. Approach to Data Protection and Privacy*, *supra* note 178 ("the law should harmonize the inconsistencies and fill the gaps created by the existing sectoral approach.").

196. *See* Houser & Voss, *supra* note 194, at 42 (discussing the U.S.'s current failure to adopt Privacy Shield protections).

In a related development, the U.S. CLOUD Act was adopted in 2018,[197] ending a dispute where Microsoft challenged Stored Communications Act (SCA) requests for access to customer electronic data held in servers in the European Union (in Ireland) up to the U.S. Supreme Court.[198] The CLOUD Act, which mooted the court case, allows the U.S. authorities to issue warrants with extraterritorial reach.[199] In July 2019, the European Data Protection Board (EDPB), the successor under the GDPR to the advisory Article 29 Working Party, which existed under the 1995 Directive,[200] and the European Data Protection Supervisor (EDPS) sent a letter to the LIBE Committee of the European Parliament, attaching as annex a legal assessment "on the impact of the US Cloud Act on the European legal framework for personal data protection."[201] The analysis indicated that the normal channel for transmission of such information was the Mutual Legal Assistance in Criminal Matters Treaty (MLAT) between the European Union and the United States, and that the CLOUD Act was likely to bypass the MLAT.[202] The position of the EDPB and the EDPS was that data subjects could only be protected by an international agreement such as a MLAT, and that the data be disclosed only in compliance with EU law, under the supervision of EU courts, and that under Article 48 of the GDPR a foreign court order to transfer data must be under an international agreement such as the MLAT in order to be recognized (that is, to be considered a lawful basis for such transfer under Article 6(1) of the GDPR).[203]

Furthermore, the legal assessment affirms that "international agreement containing strong procedural and substantive fundamental rights safeguards appears the most appropriate instrument to ensure the necessary level of protection for EU data subjects and legal certainty for businesses,"[204] and points

197. Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 18 U.S.C.A. §§ 2703, 2713.

198. *See* DEPT. OF JUST., PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 7 n.4, (2019) (discussing the outcome of *Microsoft v. United States*).

199. *See* Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1683–84 (2018) (stating "[i]n a dramatic turn of events regarding this statute, the highly contested case of United States v. Microsoft Corp. reached the Supreme Court, only to be mooted when Congress swiftly enacted the CLOUD Act of 2018. This Act settled the question of the international reach of a single U.S. legal statute: It makes clear that SCA warrants have an extraterritorial reach" (citation omitted)).

200. *Glossary-A*, EUROPEAN DATA PROTECTIONS SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/glossary/a_en.

201. Letter from Andrea Jelinek, for the EDPB, and Giovanni Buttarelli, for the EDPS, to Mr. Juan Fernando López Aguilar, Chair of the Eur. Parliament's Comm. on Civil Liberties, Just. and Home Affairs (LIBE) (July 10, 2019), https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en [hereinafter, the CLOUD Act Letter].

202. Annex: Initial Legal Assessment of the Impact of the US CLOUD Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence (July 10, 2019), https://edpb.europa.eu/our-work-tools/our-documents/letters/epdb-edps-joint-response-libe-committee-impact-us-cloud-act_en [hereinafter, Annex to the CLOUD Act Letter].

203. *See id*. at 3 (highlighting that "[u]nlike the EU Directive, the GDPR explicitly governs orders from foreign judiciaries to produce evidence regarding the personal information of EU citizens."); *see also* Samantha Cutler, Note, *The Face-Off Between Data Privacy and Discovery: Why U.S. Courts Should Respect EU Data Privacy Law When Considering the Production of Protected Information*, 59 B.C. L. REV. 1513, 1521 n.64 (2018) (referring to Article 48 of the GDPR). Note that the reference to "EU citizens," is misleading in the sense that the GDPR here refers only to personal data, so this would entail the production of personal data coming from the European Union to the United States, presumably regardless of the citizenship of the data subject.

204. *Id*. at 8.

out that some Member State blocking statutes may prevent disclosure of information by service providers to the United States, and thus may conflict with the CLOUD Act.[205] The legal assessment also refers to the EDPS opinion on the Commission's recommendation to authorize the opening of negotiations aimed at reaching an EU-US international agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters, highlighting that "[i]n order to comply with EU primary law, the conclusion of an international agreement must in any case provide for appropriate safeguards for transfers and ensure that enforceable data subject rights and effective remedies for data subjects are available."[206] While not at the heart of this study's discussion of harmonization of data privacy law in a business context, these developments and the ensuing negotiations should be seen as affecting transatlantic transfers of personal data by service providers in the context of criminal matters, and also potentially portending GDPR liability for U.S. service providers transferring personal data from the European Union to the United States in compliance with the CLOUD Act.[207]

II. OBSTACLES TO DATA PRIVACY LAW HARMONIZATION

Where convergence once reigned, divergence now stands. Accompanying this change, there have been the development of certain obstacles to true harmonization of data privacy law between the United States and the European Union identified by this study. *Laissez-faire* policy in the United States

205. *Id.* For an interesting discussion of blocking statutes or "blocking provisions," written prior to the adoption of the CLOUD Act; *see* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179, 195–98 (2018) (discussing how the United States also employs such blocking provisions).

206. *Id.* at 9–10; *see also Opinion 2/2019, EDPS Opinion on the Negotiating Mandate of an EU-US Agreement on Cross-Border Access to Electronic Evidence*, EUR. DATA PROT. SUPERVISOR 5 (Apr. 2, 2019), https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf (discussing the opening of negotiations between the EU and US) (offering the recommendations and thoughts of the EDPS relating to the Commission's recommendation to authorize the opening of negotiations aimed at reaching an EU-US international agreement on cross-border access to electronic evidence for judicial cooperation in criminal matters). For the Commission's recommendation, *see Recommendation for a Council Decision Authorising the Opening of Negotiations in View of an Agreement Between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters*, EUROPEAN COMMISSION 6 (Feb. 5, 2019), COM(2019) 70 final, https://ec.europa.eu/transparency/regdoc/rep/1/2019/EN/COM-2019-70-F1-EN-MAIN-PART-1.PDF (stating, in part, that "[t]he agreement should complement the EU-U.S. Data Protection and Privacy Agreement, otherwise known as the "Umbrella Agreement" which entered into force on 1 February 2017 and the U.S. Judicial Redress Act (JRA), extending the benefits of the U.S. Privacy Act to EU citizens that was adopted by the United States Congress on 24 February 2016," and recognizing that the "[p]ersonal data covered by this recommendation for a Council decision is protected and may only be processed in accordance with the General Data Protection Regulation (GDPR) and for authorities in the European Union, the Data Protection Directive for Police and Criminal Justice Authorities (Law Enforcement Data Protection Directive)" (citations omitted)). The Council of the European Union adopted the Council Decision Authorising the Opening of Negotiations with a View to Concluding an Agreement Between the European Union and the United States of America on Cross-Border Access to Electronic Evidence for Judicial Cooperation in Criminal Matters on June 6, 2019. *See generally Outcome of Proceedings 10128/19*, COUNCIL OF THE EUROPEAN UNION (June 12, 2019), https://data.consilium.europa.eu/doc/document/ST-10128-2019-INIT/en/pdf (discussing the reason the council came to this decision).

207. *See generally* Philippe Heinzke & Lennart Engel, *EDPB Rules on the CLOUD Act: Restrictive Position on the Legitimacy of Data Transfers to US Investigating Authorities*, C/M/S LAW-NOW (July 30, 2019), https://www.cms-lawnow.com/ealerts/2019/07/edpb-rules-on-the-cloud-act-restrictive-position-on-the-legitimacy-of-data-transfers?cc_lang=en. (discussing EDPB rules regarding the CLOUD Act).

(sometimes discussed as "neoliberalism") has rendered regulatory solutions to data privacy concerns anathema there, as discussed in Section A. Differences in lobbying and the economic and political force of the U.S. tech behemoths and advertising trade associations in the United States have been factors that, when teamed up, have led to the blocking of data privacy legislation in the United States, as detailed in Section B, while the European Union has embraced reform strengthening data privacy rights of individuals. Differing constitutional provisions have made certain EU innovations, such as the right to delisting (right to be forgotten), inimitable in the United States, as shown in Section C. As will be indicated here and there, these three obstacles are often connected.

A. Laissez-Faire Policy and Neoliberalism as an Obstacle

Laissez-faire is defined as "a doctrine opposing governmental interference in economic affairs beyond the minimum necessary for the maintenance of peace and property rights."[208] The ideology, which was the economic policy of the United States under President McKinley, was rejected after his death in 1901 by his successor, Theodore Roosevelt,[209] and would not predominate again for many decades thereafter.[210] Although "bureaucracy bashing" had already started during the administration of U.S. President Jimmy Carter,[211] the election in 1980 of U.S. President Ronald Reagan ushered in a new era of de-regulation and *laissez-faire* policy toward business.[212] This new attitude in Washington also coincided with changes in antitrust policy, that had commenced in the 1970s, as remarked by former Chair of the Board of Governors of the Federal Reserve System Alan Greenspan in 1998:

> In the 1970s and 1980s, there was a significant shift in emphasis from a relatively deterministic antitrust enforcement policy to one based on the belief (under the aegis of the so-called Chicago School) that those market imperfections that are not the result of government subsidies, quotas or franchises, would be assuaged by heightened competition. Antitrust initiatives were not seen as a generally successful remedy.[213]

Policy advocate and Columbia University Law School professor, Tim Wu, comments that antitrust law "does strike at the root cause of private political

208. *Laissez-faire*, MERRIAM-WEBSTER (last visited on Aug. 22, 2019), https://www.merriam-webster.com/dictionary/laissez-faire.

209. *See* TIM WU, THE CURSE OF BIGNESS 45–47 (2018) (discussing Roosevelt's rejection of the laissez-faire ideology).

210. *Id.*

211. *See* Karen Yeung, *The Regulatory State*, *in* THE OXFORD HANDBOOK OF REGULATION 64, 73 (Robert Baldwin, Martin Cave & Martin Lodge, eds., 2010) (describing such "bashing" as "fueling a strong push for administrative reform").

212. *See, e.g.*, Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 615 (1995) (discussing strong American beliefs in freedom from regulation, Reagan's view of himself as being empowered to stop government regulation, and the lingering view years after the Reagan presidency of regulation as "only an exception").

213. Alan Greenspan, *The Effects of Mergers (Testimony of Chairman Alan Greenspan Before the Committee on the Judiciary, U. S. Senate, June 16, 1998)*, THE FEDERAL RESERVE BOARD 4 (June 16, 1998, 10:00 AM), https://www.federalreserve.gov/boarddocs/testimony/1998/19980616.htm. For additional citations of this passage. *See also Light Touch Antitrust in* ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION 22 (2016) (highlighting ineffectiveness in antitrust initiatives).

power—the economic concentration that facilitates political action."[214] Presumably, according to Wu's logic, the changes to antitrust policy allowed for the development of the hegemonic "GAFAM" U.S. tech giants (including Google, Apple, Facebook, Amazon, and Microsoft), unconstrained by antitrust law, and permitted increased lobbying action by them.[215] Indeed, Facebook made sixty-seven unchallenged acquisitions, Amazon ninety-one, and Google 214 (although some with conditions),[216] resulting in concentration in their sectors, consolidation of their positions, and elimination of competitors. Furthermore, the *laissez-faire* ideology, which has been described as a cousin to the ideology of social Darwinism,[217] also happens to parallel the views toward regulation of many present or past libertarian-minded leaders of Silicon Valley.[218] Libertarians believe that letting markets alone will be conducive to growth and higher standards of living,[219] however, they strangely show "insensitivity to private intrusions on human freedoms,"[220] among which the right to privacy interests us. Yet, Professor Paul Ohm argues that an important value is "a bias against regulation," and that if there are other ways to prevent privacy harms—such as through technology, markets, and social institutions—"we should resist the temptation to intervene legally," while defending this path against eventual claims of "unthinking libertarianism."[221] The result is that the United States has taken a market-based approach to data privacy, in contrast to the rights-based approach of Europe.[222]

214. WU, *supra* note 209, at 23.

215. *See infra* Part II.B.3 (discussing "GAFAM" and lobbying).

216. WU, *supra* note 209, at 123.

217. *Id.* at 45.

218. PayPal co-founder Peter Thiel slipped his opinion on regulation into a discussion of biotech. "It's easy for libertarians to claim that heavy regulation holds biotech back—and it does . . . . " PETER THIEL, ZERO TO ONE 76 (2014). Ex-Google CEO Eric Schmidt, writing with Jonathan Rosenberg, stated "[r]egulations get created in anticipation of problems, but if you build a system that anticipates everything, there's no room to innovate." ERIC SCHMIDT & JONATHAN ROSENBERG, HOW GOOGLE WORKS 254–55 (First Trade Paperback ed. 2017). Earlier, Schmidt had written about fending off regulation: "Technology corporations will have to more than live up to their privacy and security responsibilities if they want to avoid unwanted government regulation that could stifle industry dynamism." ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE 66 (First Vintage Books ed. 2014). Google CEO Larry Page and co-founder Sergey Brin are reported to exhibit "contempt for law and regulation." *See* ZUBOFF, *supra* note 184, at 105. Zuboff comments that in 2013, Page "complained that "old institutions like the law" impede the company's freedom to "build really great things[.]" *See* Shoshana Zuboff, *It's Not That We've Failed to Rein in Facebook and Google. We've Not Even Tried*, THE GUARDIAN (July 2, 2019, 06:00 BST), https://www.theguardian.com/commentisfree/2019/jul/02/facebook-google-data-change-our-behaviour-democracy. Former CEO-founder of AdGrok and former product manager for Facebook Antonio García Martínez said, "For my entire career at Facebook, I was embroiled in a rolling debate with the Facebook privacy and legal teams about what we could and couldn't get away with, chiseling away at their legal trepidation, and trying to find some legal rubric that would forgive (or at least defensibly excuse) our next depredation with user data." ANTONIO GARCÍA MARTÍNEZ, CHAOS MONKEYS 317 (2016). In each case, regulations are treated as spoilers.

219. *See* ADAM WINKLER, WE THE CORPORATIONS 140 (2018) ("[l]ike modern-day libertarians . . . believed that leaving markets alone would produce a higher standard of living for more Americans.").

220. WU, *supra* note 209, at 41.

221. Ohm views this choice, instead, as representing "a more modest recognition of the "second best" nature of legal solutions." *See* Ohm, *supra* note 27, at 1177 (setting out these comments in the third step—Nonlegal Responses and Remediation—of a proposed four-step threat model for privacy harm.).

222. Reidenberg, *supra* note 105, at 782.

The American adoption of the ideology of *laissez-faire* has been revived in "neoliberalism,"[223] and in many senses the latter concept has been used to describe a conflict between market or capitalist imperatives and democratic ones,[224] such as market or self-regulation elements *versus* the adoption of statutes to regulate aspects of the economy or economic life. It harkens back to the *Lochner* era "affair" of the U.S. Supreme Court with economic libertarianism, during the period of which (roughly from the 1880s through the 1930s) the court "struck down more than 200 pieces of state and federal legislation as violations of "economic liberty" and laissez-faire policy."[225] A parallel has been drawn to today's "neoliberal constitutionalism," focused on forms of autonomy such as selling data.[226]

The move toward a *laissez-faire* policy really took hold during the Reagan administration, however, with government institutions considered necessary evils and government interference seen as causing more harm than good.[227] As Professors Ezrachi and Stucke state succinctly, "regulation has fallen on hard times."[228] It also resulted in the frustration of efforts to introduce privacy legislation in Congress.[229] As put by one commentator, "[t]he election of Ronald Reagan as President marked the end of any significant privacy policy initiatives from the executive branch," and this frustration resulted in divergence with other Western industrialized countries on privacy.[230] Indeed, compared to the period that preceded him, "President Ronald Reagan's approach to privacy was less accommodating, and certainly not enthusiastic"[231] and proposals contained in a 1977 report by the Privacy Protection Study Commission (PPSC), set up under the 1974 Privacy Act[232] in order to evaluate the statute and recommend improvements to it, "were not carried out."[233] Moreover, Reagan's policy bent resulted in a rejection of President Jimmy Carter's intention that the United

223. Neoliberalism has been explained to refer "to the revival of the doctrines of classical economic liberalism, also called laissez-faire, in politics, ideas, and law." It involves "the intensification of a familiar and longstanding "anti-regulatory" politics" (citation omitted). David Singh Grewal & Jedediah Purdy, *Introduction: Law and Neoliberalism*, 77 LAW & CONTEMP. PROBS. 1, n.1 (2014). As such, it fits perfectly with the use made in this study of the term "*laissez-faire*."

224. *Id.* at 2–3.

225. *See* Jedediah Purdy, *Neoliberal Constitutionalism: Lochnerism for a New Economy*, 77 LAW & CONTEMP. PROBS. 195, 196–97 (2014) (discussing new Lochnerism and its origins).

226. *Id*. at 197.

227. *See* EZRACHI & STUCKE, *supra* note 213, at 25 (citation omitted).

228. *Id*. at 23.

229. *See* John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 997–998 (1984) (highlighting the failure of the Office of Management and Budget, the director of which is appointed by the President, to introduce legislation for the supervision of agency procedures in the area of privacy, as well as Reagan Administration actions to loosen privacy protection of tax and debt records held by the government).

230. Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 202 (1993) (at the time of writing the article, Gellman was Chief Counsel, Subcommittee on Information, Justice, Transportation, and Agriculture, House Committee on Government Operations).

231. Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 900 (2013).

232. Privacy Act of 1974, 5 U.S.C. §552a (2012).

233. Clearwater & Hughes, *supra* note 231, at 900.

States should adopt the OECD Privacy Guidelines,[234] which are discussed in Part I.A.2.

This *laissez-faire* policy is reflected today in the self-regulatory nature of U.S. data privacy,[235] outside of applicable sectoral law provisions. This approach has been favored by the FTC and the U.S. Department of Commerce and usually involves industry groups adopting voluntary codes of conduct.[236] Critics have seen this approach as a failure "due to an overall lack of accountability and transparency, incomplete realization of robust privacy principles, free rider issues, and weak oversight and enforcement," the goal of which they have seen as avoiding government regulation.[237] Such self-regulation has been described as the firms taking on the regulatory functions that are normally the purview of the government, with several perverse effects, including lack of accountability to the government, and no dispute resolution mechanism, among others.[238] Perhaps intuitively, this self-regulation has been backed by business interests.[239] The people's representatives in government and the data subjects, then, are absent from the self-regulatory process. Certain authors today see that such self-regulation in the area of privacy has failed.[240] The *laissez-faire* policy described above may also be seen as reflected by the relatively lax enforcement practices of the FTC.[241] In a nutshell, the European Data Protection Supervisor explained the U.S. situation as follows: "the United States, where in the name of free markets, data is another locus for competition between companies and consumers," contrasted with the fundamental rights basis for data protection in Europe,[242] which is discussed in Section C.

---

234. *Id*. at 903 (footnote omitted).

235. *See, e.g.*, Lilian Edwards, *Reconstructing Consumer Privacy Protection On-Line: A Modest Proposal*, 18 INT'L REV. L. COMPUTERS & TECH. 313, 316 (2004) (commenting that in comparison to the European Union, "in the USA the legal culture has historically been very different, with the regime in relation to private collectors of data (as opposed to the state) one of industry self-regulation and a *laissez-faire* attitude to legal regulation in this area.").

236. *Id.* at 337 n.2, 343 n.104.

237. Rubinstein, *supra* note 56, at 1 (footnote omitted).

238. *Id*. at 3 ("Thus, participating firms are accountable to each other or the trade association but not directly to the government; they engage in rulemaking consensually by members who adopt the code; there is neither adjudication (except perhaps by a peer review committee) nor a dispute resolution mechanism, and only limited sanctions apart from ejection of noncompliant firms from the trade association; and coverage of relevant industry principles suffers from free rider problems due to the voluntary nature of the regulatory regime. Finally, there is little public involvement, although firms developing a code may engage in public consultation at their discretion." (footnote omitted)).

239. *See* BENNETT & RAAB, *supra* note 20, at 131 ("Influential business and government interests in North America, and frequently in other places, have tended to argue that comprehensive, general privacy laws are unnecessary, and that privacy can be better protected at the *sectoral* level, when and if necessary, or through self-regulation." (citation omitted)).

240. *See, e.g.*, Rubinstein, *supra* note 56, at 2 ("self-regulation in the form of voluntary codes has had a sufficiently long run to prove its worth but has failed."); *see also* Gellman & Dixon, *supra* note 156, at 74 ("Privacy self-regulation has generally failed when industry acts by itself behind closed doors."). For an earlier view, *see* Chris Jay Hoofnagle, *Privacy Self Regulation: A Decade of Disappointment*, ELECTRONIC PRIVACY INFORMATION CENTER at 15 (Mar. 4, 2005), https://epic.org/reports/decadedisappoint.pdf ("Ten years of self-regulation has led to serious failures in this field.").

241. For a discussion on the role of the FTC, *see supra* Part I.B.3.

242. Giovanni Buttarelli, European Data Protection Supervisor, Youth and Leaders Summit – Opening Speech at 2 (Jan. 19, 2019), https://edps.europa.eu/sites/edp/files/publication/19-01-21_speech_youth_and_leaders_en.pdf.

Thus, the possibilities for harmonization of law, including through its proper application, appear to be limited by the *laissez-faire* approach of the United States and its top privacy regulator. Laws are not adopted, for fear of braking technological or economic progress, or just on ideological grounds. Self-regulation is preferred to legislation, in a way that is the opposite of the path taken in the European Union, with the adoption of the GDPR and its grant of greater powers for independent data privacy authorities there. Lobbying might continue to block the adoption of legislation in the United States, or at least reduce the chance for true harmonization of laws between the United States and the European Union.

B. Lobbying as an Obstacle

Lobbying comes from the verb, "to lobby," which means "to conduct activities aimed at influencing public officials and especially members of a legislative body on legislation."[243] This study will first explicate differences between lobbying in the United States and Europe, on one hand, and between U.S. and European companies, on the other hand in Section 1, before tracing a brief historical view of lobbying on data privacy law and regulation in Section 2. Finally, a forward-looking discussion on why lobbying is an obstacle to harmonization concludes this Part II.B. in Section 3.

1. Differences in Lobbying: United States/European Union; U.S. Companies/European Companies

Differences in lobbying between the United States and the European Union might help explain in part why today the United States has no general data privacy legislation and the European Union does, despite the massive lobbying of U.S. tech companies during the European Union legislative procedure leading up to the adoption of the GDPR.[244] Professor Christine Mahoney argues that a major difference between lobbying in the United States and the European Union is that the United States has failed to adopt "real campaign-finance reform," and that unlike the United States, in the European Union, most policymakers are not elected and thus, do not need to finance expensive election campaigns. This, in

243. *Lobby*, MERRIAM-WEBSTER (last visited on Aug. 21, 2019), https://www.merriam-webster.com/dictionary/lobbying.

244. The GDPR itself has been described as "one of the most lobbied pieces of European legislation in European Union history." *See* Ece Özlem Atikcan & Adam William Chalmers, *Choosing Lobbying Sides: The General Data Protection Regulation of the European Union*, J. PUBL. POL'Y 1, 3 (2018) (citation omitted) (describing a scandal where European Parliament members were found cutting and pasting lobbyist texts into amendments, which "highlighted the lobbying power exerted by US internet and retail giants, like Amazon and eBay"). For the individual corporate political activity of certain U.S. tech companies on the GDPR text, see Andrew Barron & W. Gregory Voss, *La Culture et Son Impact Sur les Actions Politiques des Entreprises: Le Cas du Règlement Général Sur la Protection des Données (RGPD)* [*Culture and Its Impact on Corporate Political Activity: The Case of the General Data Protection Regulation (GDPR)*], 41 REVUE FRANÇAISE DE GESTION 109, 119 (2015). Note that Bennett and Raab also briefly discuss American lobbying efforts on the GDPR's predecessor, the 1995 Directive, and the DPA's efforts together, on the other side. Bennett and Raab, *supra* note 20, at 94–95.

turn, allows them to take more principled stances in policymaking.[245] She also found that most often in the United States, industry and business lobbyists (corporations and trade associations) achieved success, while "those fighting for the broader good" (citizen groups and foundations) fail, whereas policy outcomes in the European Union were more balanced.[246]

The situation in the European Union is made possible because the Commission, which represents the interests of the European Union, is the only institution that may propose legislation to the European Parliament (Parliament) and the Council of the European Union (Council).[247] The Commission is accountable to the Parliament and appointed by the Council with the consent of the Parliament, with its President elected by the Parliament.[248] Another difference between the European and U.S. legislative processes is that the former have more analytical and procedural requirements, whereas in the United States legislative proposals may originate from a multitude of sources, such as lobbyists.[249] In the United States, most of the action regarding proposed legislation occurs out of the view of the public, off the Congressional floor, "in lobbies and antechambers" where lobbyists and legislative actors meet to discuss amendments and negotiate compromises.[250] Where in the United States, most bills "die at the end of a legislative session in which they were submitted," in Europe, there is a high likelihood that a legislative proposal submitted to the Parliament will become law in at least a similar form, as a result of the earlier vetting done by the Commission.[251]

The way that U.S. and Continental European companies conduct lobbying is different as well. U.S. companies carry out lobbying both individually and through trade associations.[252] European companies, on the other hand, perhaps with the exception of the English-speaking nations (including England, who will soon leave the European Union through Brexit), tend to carry out lobbying through trade associations.[253] Related to this point is the sheer economic power of U.S. tech companies, which has translated itself into large lobbying

245. Christine Mahoney, *Why Lobbying in America is Different*, POLITICO (June 4, 2009, 6:15 AM), https://www.politico.eu/article/why-lobbying-in-america-is-different/ ("[T]he majority of policymakers in the EU institutions are not elected, and since they do not need to stand for elections, they do not need to find the significant amounts of cash to support campaigns. Instead of spending innumerable hours fundraising, they balance competing interests in an effort to produce policies that are seen as legitimate, though produced by a less-than-democratic supranational structure.").

246. *Id*.

247. *See* Richard W. Parker & Alberto Alemmano, *A Comparative Overview of EU and US Legislative and Regulatory Systems: Implications for Domestic Governance & the Transatlantic Trade and Investment Partnership*, 22 COLUM. J. EUR. L. 61, 67–68 (2015).

248. *Id*.

249. *Id*. at 70.

250. *Id*. at 77.

251. *Id*. at 70.

252. Barron & Voss, *supra* note 244, at 124.

253. *Id*. One study showed that, in the case of lobbying on the GDPR, "Anglo" firms (consisting of U.S. and UK firms, in this case) showed higher levels of what the authors refer to as "corporate political activity" (CPA) compared to their Continental European counterparts (consisting of German, Nordic and Latin European country firms). The former were more likely to employ individual CPA and constituency-building strategies than the latter. *See* Barron & Voss, *supra* note 244, at 124 (demonstrating this likelihood).

budgets.[254] In addition, a subset of U.S. companies—often young innovative U.S. tech companies such as Uber—engage in what two authors call "regulatory entrepreneurship," where part of the business strategy is to change laws, potentially breaking the laws in the interim.[255] One technique of regulatory entrepreneurs is to "mobilize their users and stakeholders as a political force."[256] This may involve asking users to sign petitions or contact legislators, among other techniques.[257] However, this is not the traditional form of lobbying that has manifested itself in the area of data privacy, as shall now be seen.

2. A Brief Historical View of Lobbying on Data Privacy Legislation and Regulation in the United States

Industry lobbying on proposed data privacy legislation has a long history in the United States.[258] Even in the case of successfully-adopted legislation, however, in general, its impact has been either to block legislation or to lessen the protection provided by the legislation.[259] For example, the FCRA was "severely weakened due to the effective lobbying of the credit-reporting industry,"[260] notably allowing credit agencies to sell certain personal information from credit histories to commercial entities.[261] Shortly thereafter, the Privacy Act of 1974[262] was subject to lobbying by the likes of banks and insurance companies, resulting in it being limited to government record-keeping.[263] Later, in the case of the GLBA,[264] lobbying resulted in a sectoral law with an "opt-out" for sharing with other companies of personal information

254. *See infra* Part II.B.3 (describing why lobbying is an obstacle to harmonization).

255. *See* Elizabeth Pollman & Jordan M. Barry, *Regulatory Entrepreneurship*, 90 S. CAL. L. REV. 383, 386 (2017) (defining "regulatory entrepreneurs" as companies that "pursue a line of business that has a legal issue at its core—a significant uncertainty regarding how the law will apply to a main part of the business operations, a need for new regulations in order for products to be feasible or profitable, or a legal restriction that prevents the long-term operation of the business." For such entrepreneurs, political activity is necessary in order to try to change or shape the law, and thus is integrated as a "major component of their business models."). *Id*. at 392.

256. *Id*. at 390.

257. *Id*. at 404.

258. *See, e.g.*, Daniel Stevens, *Chamber and Google Among Top Lobbying Spenders in First Quarter of 2015*, MAPLIGHT (Apr. 21, 2015), https://maplight.org/story/chamber-and-google-among-top-lobbying-spenders-in-first-quarter-of-2015/ (discussing data that shows Google as one of the top spenders on lobbying efforts in the first quarter of 2015).

259. *See, e.g.*, Kartikay Mehrotra, Laura Mahoney, and Daniel Stoller, *Google and Other Tech Firms Seek to Weaken Landmark California Data Privacy Law*, L.A. TIMES (Sept. 4, 2019, 2:32 PM), https://www.latimes.com/business/story/2019-09-04/google-and-other-tech-companies-attempt-to-water-down-privacy-law (discussing how Google and other industry allies are attempting to carve out exemptions for digital advertising in California's data privacy law).

260. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1440 (2001), *citing* PRISCILLA M. REGAN, LEGISLATING PRIVACY 101 (1995).

261. *Id*. at 1440–1441; *see also* Shattuck, *supra* note 229, at 996–97 (noting that the Fair Credit Reporting Act of 1970 was weakened through amendments drafted by the credit reporting industry).

262. Privacy Act of 1974, Pub. L. No. 93-579 (codified at 5 U.S.C. § 552a (2016)).

263. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 127 n.25 (2004) ("The Privacy Act of 1974 addressed only government record-keeping, bowing to the lobbying of large private record-keeping institutions (like banks and insurance companies) to remove their interests from the general privacy rights umbrella." (citations omitted)). Note that, as the Privacy Act was so limited, it became less interesting in the framework of this study, which focuses on business law.

264. Gramm-Leach-Bliley Act (Financial Modernization Act of 1999), Publ. L. No. 106-102, 113 Stat. 1338 (codified at 15 U.S.C. § 6801(2016)).

by the financial institution, effectively making sharing the default position.[265] Lobbyists succeeded in helping block a California "Right to Know" digital privacy bill aimed at data brokers in 2013.[266] An attempt by the Obama administration to adopt a consumer privacy "bill of rights," failed following extensive lobbying by organizations representing Facebook and Google.[267]

Moreover, an additional development in this area, noted at the turn of the millennium, was that trade associations were at the same time engaging in discussion on privacy issues (perhaps espousing self-regulation solutions) and lobbying against regulation.[268] This was true of a "key player"—the Direct Marketing Association (DMA)—even earlier in the 1970s.[269] It operated services to allow consumers to opt-out of direct marketing, but because of the burdensomeness of the procedures and the limited scope of the registries, these were ineffective.[270] Self-regulation measures such as these were also cited by the FTC as reasons for not recommending legislation.[271]

GAFAM members may engage in many forms of corporate political activity. Taking the example of Google, this may include traditional lobbying, a "revolving door" of personnel between the company and the administration,

265. Laura Hildner, *Defusing the Threat of RFID: Protecting Consumer Privacy Through Technology-Specific Legislation at the State Level*, 41 HARV. C.R.-C.L. L. REV. 133, 144 (2006) (stating that the author sees this as an example of Congress allowing "lobbying groups to secure limitations that partially vitiate the statutes' goal of protecting individual privacy.").

266. BYGRAVE, *supra* note 21, at 111 ("Proposed legislative measures in the field usually face strong opposition from affected business groups. The latter typically have well-oiled lobbyist machinery at their disposal, along with a considerable number of 'veto points' through which to exert pressure. A recent case in point, from May 2013, was the defeat of a bill introduced into the Californian legislature which would have given consumers a right to gain insight into their personal profiles compiled by online data brokers"). Lobbying against the "Right to Know" bill involved, among others, Google and Facebook. *See* Jessica Guynn & Marc Lifsher, *Silicon Valley Uses Growing Clout to Kill a Digital Privacy Bill*, L.A. TIMES (May 3, 2013, 12:00 AM), https://www.latimes.com/business/la-xpm-2013-may-03-la-fi-digital-privacy-20130503-story.html ("The bill faced vehement opposition from a powerful coalition of technology companies and business lobbies that included Facebook Inc., Google Inc., the California Chamber of Commerce, insurers, bankers and cable television companies as well as direct marketers and data brokers. Their members collectively give millions of dollars to lawmakers and politicians").

267. *See* Tony Romm, *The Trump Administration is Talking to Facebook and Google about Potential Rules for Online Privacy*, WASH. POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/?noredirect=on&utm_term=.55177a534e92 (commenting that "they and other tech companies warred with privacy groups"). *See* Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 378 (2015) (describing such bill, if it had been adopted, was described as "a modest first step to harmonizing U.S. privacy law with European 'mutually recognized privacy protection'").

268. *See, e.g.*, Reidenberg, *supra* note 105, at 776 (stating that the theory of self-regulation is "pure sophistry" and "hypocritical").

269. *See* Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 153–154 (describing the DMA as one of the "lobbying groups for data traders").

270. *Id*. (describing the DMA as one of the "lobbying groups for data traders"). The full name of the DMA is now Data & Marketing Association, and it has been acquired by the Association of National Advertisers (ANA); *see also*, Bob Liodice & Tom Benton, *ANA Acquires DMA, Creates Unified Voice for Advertising and Marketing Growth*, MEDIAVILLAGE.COM (July 3, 2018), https://www.mediavillage.com/article/ana-acquires-dma-creates-unified-voice-for-advertising-and-marketing-growth/. Its members include Google and Facebook. *See Data & Marketing Association*, WIKIPEDIA (last edited Sept. 4, 2019 08:3812), https://en.wikipedia.org/wiki/Data_%26_Marketing_Association (stating its members include Google and Facebook).

271. *See* Ludington, *supra* note 269, at 154 ("The FTC issued a report to Congress in 1998, concluding that commercial Web sites were not effectively regulating privacy on the Internet, but recommending against legislation because industry leaders had pledged 'their commitment to work toward self-regulatory solutions.'"(citations omitted)).

and a campaign to exert public influence that might include academic work.[272] Corporate political activity other than legislative lobbying may also impact positions held by the regulators. One trade association that has established principles for self-regulation and provides research supporting self-regulation and continuing access to advertising-sponsored free content—the Digital Advertising Alliance (DAA)—includes Google, Amazon, Facebook and Microsoft as participating companies.[273] The DAA's research "showing that 92 percent of consumers agreed that free content is important to the value of the Internet," which the organization sees as a validation of the "graduated privacy permission approach" of the DAA's self-regulation principles, was cited by the FTC in a filing with the National Telecommunications and Information Administration (NTIA).[274] The NTIA is an agency of the U.S. Department of Commerce that advises the President on telecommunications and information administrative issues,[275] and the FTC filing was in response to a NTIA request for comments "on ways to advance consumer privacy while protecting prosperity and innovation."[276] In its filing, the FTC cited the DAA's research for the proposition that certain controls by consumers over data collected about them "can be costly to implement and may have unintended consequences.[277] For example, if consumers were opted out of online advertisements by default (with the choice of opting in), the likely result would include the loss of advertising-funded online content."[278] Thus, the DAA's work has resulted in U.S. privacy regulator (FTC) cautions against "opt-in," which is a traditional element of EU data privacy law, which also is a point where harmonization might be difficult to achieve, as the regulatory approach in the U.S. is "opt-out."[279]

---

272. ZUBOFF, *supra* note 184, at 122.

273. *DAA Participating Companies & Organizations*, DIGITAL ADVERTISING ALLIANCE (last visited Aug. 21, 2019), https://digitaladvertisingalliance.org/participating.

274. Lou Mastria, *DAA, Interest-Based Advertising Cited in Federal Trade Commission Filing with National Telecommunications & Information Administration*, DIGITAL ADVERTISING ALLIANCE (Nov. 16, 2018), https://digitaladvertisingalliance.org/blog/daa-interest-based-advertising-cited-federal-trade-commission-filing-national.

275. *About NTIA*, NAT'L TELECOMM. & INFORMATIONAL ADMIN. (last visited Aug. 21, 2019), https://www.ntia.doc.gov/about.

276. *Comments on Developing the Administration's Approach to Consumer Privacy*, NAT'L TELECOMM. & INFORMATIONAL ADMIN (Nov. 13, 2018), https://www.ntia.doc.gov/other-publication/2018/comments-developing-administration-s-approach-consumer-privacy.

277. DIGITAL ADVERTISING ALLIANCE, *supra* note 274.

278. FED. TRADE COMM., Staff Comment to the National Telecommunications & Information Administration In the Matter of Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780–8780–01 (Nov. 9, 2018), at 15, https://www.ntia.doc.gov/files/ntia/publications/federal_trade_commission_staff_comment_to_ntia_11.9.2018.pdf.

279. *See* Hash, *supra* note 189, at 1063 ("The United States' regulatory approach to the use of company-collected personal data is best described as an "opt-out" standard"); *see also* Schwartz & Peifer, *supra* note 35, at 154–55 (citing GLBA as an example of an opt-out statute and commenting that "opt-out consent in the United States has not effectively protected consumer privacy rights"). Although "opt-in" does exist in the United States, its scope has been narrow. *See id*. at 153–54 (citing FCRA and the Video Privacy Protection Act as having "opt-in," but with narrow scope for this in data privacy).

Transparency about data processing is a key requirement of the GDPR.[280] Furthermore, the GDPR requires data controllers to provide a specific list of information to data subjects both where the data have been collected directly from them[281] or where the data have been collected indirectly.[282] However, in the United States, where there is little transparency over data usage and little control over service providers, companies intend on "keeping it that way" and lobby against regulation that might require transparency about data usage.[283] The U.S. sectoral system of privacy legislation has been described as "haphazard legislative coverage of personal information" resulting from a "history of effective lobbying by the direct marketing industry, which has actively worked against government regulation of data trading."[284]

At the same time, contrary to industry forces (such as those today of the huge U.S. tech companies), efforts by privacy advocates have not been effective, perhaps because privacy harms have been seen as too abstract.[285] Perhaps, too, the "nothing to hide" argument, often seen in instances of government surveillance,[286] may influence attitudes to what is now called "surveillance capitalism."[287]

3. Forward-Looking: Lobbying as an Obstacle to Harmonization

Lobbyists are already helping shape the law in what has been called the "platform economy."[288] With the huge tech companies in the United States, there is a concentration of economic power that translates into lobbying power as well. The five largest U.S. firms by market capitalization were all in the sector

280. Transparency about processing is a data protection principle under the GDPR. Personal data is to be "processed lawfully, fairly and in a transparent manner in relation to the data subject . . . ." GDPR, *supra* note 16, at art. 5(1)(a).

281. These include the identity and contact details of the controller, and where applicable, the data protection officer, the purposes and legal basis for the data processing, the recipients of the personal data, if any, the period of data storage or criteria used to determine such period, the existence of various rights, etc. *Id*. at art. 13.

282. *Id*. at art. 14.

283. *See* Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 5–6 (2018) (citing the case of Walmart spending $34 million on lobbying over five years in the area of privacy legislation).

284. Ludington, *supra* note 269, at 153.

285. Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future*, 105 NW. U. L. REV. 1153, 1201 (2011) ("The privacy field has been ineffective in part because its narrative about the harms of sorting and the digital dossier is too abstract to whip up any legislative or public response. The threat has seemed intangible—the prospect of data aggregators targeting consumers for certain products or more accurately assessing credit risks may not be concrete enough to make legislators take notice. More bluntly, such descriptions of the digital dossier's harms may simply not be enough to counter the power lobbying voices of the firms and industries that benefit from increased sorting accuracy").

286. *See* DANIEL J. SOLOVE, NOTHING TO HIDE 21–37 (2011).

287. *See* Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75 (2015) (describing surveillance capitalism as a "new form of information capitalism" that "aims to predict and modify human behavior as a means to produce revenue and market control," and which results from a "deeply intentional and highly consequential new logic of accumulation," of which big data is a "foundational component.").

288. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. Davis L. Rev. 133, 136 (2017) (commenting that "Law for the platform economy is already being written—not via discrete, purposive changes, but rather via the ordinary, uncoordinated but self-interested efforts of information-economy participants and the lawyers and lobbyists they employ").

of information technology and Internet (including e-commerce and social media) at October 24, 2017: (in order) Apple, Alphabet (Google), Microsoft, Facebook, and Amazon.[289] Ironically, there have been claims that the GDPR has strengthened one of these firms—Google—in the area of online advertising.[290] Facebook and Amazon have also seen their online advertising market share increase.[291]

These five tech firms (which this study will refer to by the acronym used by many Europeans for them, taking the first letter of their respective names—GAFAM)[292] have been heavily engaged in lobbying and other political activities on various issues of interest to them: corporate tax rates and President Trump's immigration ban;[293] net neutrality, online piracy laws, and cable set-top box reforms;[294] government procurement, antitrust, and sales tax on online transactions[295] figure among these. As an example, Facebook has been active in (and successful) in lobbying to prevent or weaken state biometrics legislative proposals.[296]

289. Kenneth Kiesnoski, *The Top Ten US Companies by Market Capitalization*, CNBC (Mar. 8, 2017, 7:53 AM), https://www.cnbc.com/2017/03/08/the-top-10-us-companies-by-market-capitalization.html. These firms were also the largest global companies by market capitalization in August 2017 according to Nobel Prize-winning economist Jean Tirole, who also describes them as "two-sided platforms," a business model that also characterizes "[s]even of the ten largest startups." TIROLE, *supra* note 33, at 379. By March 29, 2019, the order of the companies had shifted to Microsoft, Apple, Amazon, Alphabet (Google), followed by a non-GAFAM company—Berkshire Hathaway—at fifth place, and Facebook at sixth place. *See Largest U.S. Corporations*, FORTUNE, June 2019, at F1–F4 (sorting by market value of companies as of March 29, 2019).

290. "In an industry heavily reliant on collecting data from internet users, the market share of Google, which was already the largest player, has increased as publishers became increasingly reliant on the search giant's GDPR-compliant services….". *See* Mark Scott, Laurens Cerulus & Laura Cayali, *Six Months in, Europe's Privacy Revolution Favors Google, Facebook*, POLITICO (Nov. 23, 2018 2:45 PM), https://www.politico.eu/ article/gdpr-facebook-google-privacy-data-6-months-in-europes-privacy-revolution-favors-google-facebook/. For another view that Facebook and Google could benefit from the GDPR, see Daisuke Wakabayashi & Adam Satariano, *How Facebook and Google Could Benefit From the G.D.P.R., Europe's New Privacy Law*, N.Y. TIMES (Apr. 23, 2018), https://nyti.ms/2HpH9Nl.

291. Scott et al., *supra* note 290.

292. *See* W. Gregory Voss, *Internet, New Technologies, and Value: Taking Share of Economic Surveillance*, 2017 U. ILL. J.L. TECH. & POL'Y 469, 474 (2017) (explaining how the origin of GAFAM comes from French technology scholars).

293. Elizabeth Dwoskin & Todd C. Frankel, *Silicon Valley is Debating How Far to Go to Fight Donald Trump's Executive Order*, WASH. POST (Jan. 29, 2017, 8:32 PM), https://www.washingtonpost.com/business/silicon-valley-is-debating-how-far-to-go-to-fight-donald-trumps-executive-order/2017/01/29/3a471d17-e667-4bca-84f6-d2d5c99ab12a_story.html; *see also* Ashley Carman, *Microsoft Joins Amazon in Lawsuit Over Trump's Immigration Ban*, THE VERGE (Jan. 30, 2017, 7:26 PM), https://www.theverge.com/2017/1/30/14447166/microsoft-amazon-washington-trump-immigration-ban-lawsuit ("Now, at least three tech companies—Microsoft, Amazon, and Expedia—are joining that legal fight.").

294. Cecilia Kang, *Google, in Post-Obama Era, Aggressively Woos Republicans*, N.Y. TIMES (Jan. 27, 2017), https://nyti.ms/2jFec07 ("Obama also repeatedly supported proposals backed by Google, including net neutrality in 2015 and cable set-top box reforms [in 2016] . . . .").

295. Ben Brody, *Amazon Lobbying Reaches Company Record Amid Pentagon Competition*, BLOOMBERG (Oct. 23, 2018, 8:50 PM), https://www.bloomberg.com/news/articles/2018-10-23/amazon-lobbying-reaches-company-record-amid-pentagon-competition ("Amazon also faced the tax implications of a U.S. Supreme Court ruling in June that opened the door for state and local governments to pursue sales taxes on more online transactions.").

296. ZUBOFF, *supra* note 184, at 252. Note that there are no current federal statutes "protecting or regulating the collection or commercial use of biometric identifiers, and only limited state protections." (citation omitted). Carra Pope, *Biometric Data Collection in an Unprotected World: Exploring the Need for Federal Legislation Protecting Biometric Data*, 26 J.L. & Pol'y 769, 770 (2018).

According to the Center for Responsive Politics, on the 2018 top twenty list for spending on lobbying were: Alphabet, Google's parent, at eighth place, with expenditures of $21,770,000; Amazon.com, at thirteenth place, with expenditures of $14,400,000; and Facebook Inc, at eighteenth place, with expenditures of $12,620,000.[297] Further down in the second twenty was Microsoft, at thirty-sixth, with lobbying expenditures in 2018 of $9,590,000[298] and Apple trailed with $6,680,000 in lobbying expenditures.[299] Moreover, at least one trade association of which a GAFAM company is a member figures on the list, too: the Business Roundtable, of which Amazon and Apple are members,[300] placed seventh, with expenditures of $23,160,000,[301] and a smaller association—Internet Assn—that includes Google, Amazon, Facebook and Microsoft,[302] had expenditures of $2,600,000 in 2018.[303] Furthermore, the trend has been for greater lobbying expenditure by the GAFAM, especially when measured since 2008 (which ended a relatively stable period).[304] Given the financial position of the GAFAM, there is nothing to indicate a slow-down in such spending, which gives the GAFAM political clout.

Since the passage of the California Consumer Privacy Act (CaCPA),[305] tech companies have called for federal privacy legislation. CaCPA, which has been described as a "bombshell," has confronted tech companies with the possibility of "disparate data privacy rights rules across different states," triggering calls for federal legislation.[306] However, these should not be seen as something that indicates that the lobbying obstacle has now become something quite the opposite. Instead, as Professor Paul Schwartz predicted more than ten

297. Center for Responsive Politics, *Top Spenders - 2018*, OPENSECRETS.ORG (last visited Aug. 20, 2019), https://www.opensecrets.org/lobby/top.php?showYear=2018&indexType=s.

298. Center for Responsive Politics, *Microsoft Corp - Profile for 2018 Election Cycle*, OPENSECRETS.ORG (last visited Aug. 20, 2019), https://www.opensecrets.org/orgs/summary.php?id=D000000115.

299. Center for Responsive Politics, *Apple Inc - Client Profile: Summary, 2018*, OPENSECRETS.ORG (last visited on Aug. 20, 2019), https://www.opensecrets.org/lobby/clientsum.php?id=D000021754.

300. *Members*, BUSINESS ROUNDTABLE (last visited on Aug. 20, 2019), https://www.businessroundtable.org/about-us/members.

301. *Top Spender – 2018*, *supra* note 297. Note that one or more of the GAFAM may be members of the U.S. Chamber of Commerce—the largest spender on the list—but this is uncertain given that the U.S. Chamber of Commerce does not reveal the identities of its members. *Frequently Asked Questions—#1*, U.S. CHAMBER OF COMMERCE (last visited Aug. 20, 2019), https://www.uschamber.com/about-us/about-the-us-chamber/frequently-asked-questions#1. However, it is known that Apple left the U.S. Chamber of Commerce in 2009. *See* Jim Snyder, *Apple Leaves U.S. Chamber Over Stance on Climate Change Bill*, THEHILL.COM (Oct. 6, 2009), https://thehill.com/homenews/news/61669-apple-becomes-fourth-company-to-leave-us-chamber (reporting an official statement from Apple announcing they are leaving the U.S. Chamber of Commerce).

302. *Our Members*, INTERNET ASSOCIATION (last visited Aug. 20, 2019), https://internetassociation.org/our-members/.

303. Center for Responsive Politics, *Internet Assn – Client Profile: Summary, 2018*, OPENSECRETS.ORG (last visited Aug. 20, 2019), https://www.opensecrets.org/lobby/clientsum.php?id=D000067668&year=2018.

304. Center for Responsive Politics, *Amazon.com—Profile for 2018 Election Cycle*, OPENSECRETS.ORG (last visited Sept. 15, 2019); *supra* note 299; Center for Responsive Politics, *Facebook Inc.—Client Profile: Summary*, OPENSECRETS.ORG (last visited Sept. 15, 2019); *supra* note 298.

305. California Consumer Privacy Act of 2018 ("CaCPA"), Cal. Civ. Code § 1798.198(a) (2018).

306. David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law/.

years ago, this may be an effort to preempt the state legislation.[307] The likely goal, at least in the case of the CaCPA, is to mitigate the effect of the relatively broad state legislation through weaker federal provisions. One campaigner who helped pass CaCPA described the change in attitude of tech companies: "A year ago, their playbook was self-regulation" . . . . "But now, they want a federal law that is weak."[308] Lobbying would thus still be an obstacle to harmonization.[309] The sale of data has become too important to the internet economy to make any meaningful privacy law reform likely.[310] Furthermore, given their business models, the GAFAM should not be expected to lobby for an end to commercial surveillance.[311] It is likely their arguments for a weak federal law will include those brought by the Information Technology & Innovation Foundation (ITIF), self-described as "the world's leading think tank for science and technology policy,"[312] reported to have as members GAFAM companies Google, Amazon and Microsoft.[313] In a report, ITIF claims that Congress's key task in establishing new federal data privacy legislation will "not be to maximize consumer privacy, but rather to balance competing goals such as consumer privacy, free speech, productivity, U.S. economic competitiveness, and innovation," and specifically criticizes the alleged "steep cost" of the GDPR, in terms of compliance costs and brakes on innovation.[314] If these arguments prevail, there will certainly be no true harmonization between any new U.S. federal data privacy law, and the GDPR so criticized.

In any event, the GAFAM will have their say in any attempt at data privacy harmonization. U.S. Rep. Hank Johnson from Georgia, who has proposed data

307. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 946 (2008) ("State innovations in the information privacy field are also likely to provoke industry lobbying for federal responses. There will likely be many attempts, including some successful ones, at defensive preemption in federal sectoral privacy law.").

308. Mark Scott, *Apple, Google, Facebook Line up to Pay Homage to EU Privacy Rules*, POLITICO (Oct. 26, 2018, 3:08 AM), https://www.politico.eu/article/europe-privacy-apple-google-facebook-line-up-to-pay-homage-to-rules/ (reporting that advocates are warning that tech firms want new legislation "so that they can lobby to water it down as much as possible").

309. Indeed, U.S. businesses have been "pushing the Trump administration to articulate a vision of privacy that's less aggressive than that of Europe." Romm, *supra* note 267.

310. *See* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. 667, 702 (2017) (explaining that Congress' priorities are on privacy in the national security space, which means privacy in the commercial space will not likely see reform soon).

311. Harvard Business School professor emerita Shoshana Zuboff described the situation this way: "Demanding privacy from surveillance capitalists," says Zuboff, "or lobbying for an end to commercial surveillance on the internet is like asking old Henry Ford to make each Model T by hand. It's like asking a giraffe to shorten its neck, or a cow to give up chewing. These demands are existential threats that violate the basic mechanisms of the entity's survival." John Naughton, *'The Goal is to Automate Us': Welcome to the Age of Surveillance Capitalism*, GUARDIAN (Jan. 20, 2019), https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

312. Lindsay Bednar, *ITIF Ranked World's Top Think Tank for Science and Tech Policy*, INFO. TECH. & INNOVATION FOUND. (Feb. 2, 2018), https://itif.org/publications/2018/02/02/itif-ranked-worlds-top-think-tank-science-and-tech-policy.

313. *See* Jared McDaniel, *A Grand (One Sided) Bargain*, N.C. J.L. & TECH. (Jan. 28, 2019), http://ncjolt.org/a-grand-one-sided-bargain/ (reporting on the think-tank ITIF's proposal for preemptive federal data privacy legislation).

314. ALAN MCQUINN & DANIEL CASTRO, A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA 2–3 (2019), http://www2.itif.org/2019-grand-bargain-privacy.pdf?_ga=2.136933939.241120751.1550401123-319929087.1550401123.

protection regulation, is reported to have stated, "I fully expect that Congress would seek input from Silicon Valley in creation of new regulations to create transparency and control for consumers over their personal data online;" and this might lead to a lobbying battle.[315] Thus GAFAM input is made both through traditional lobbying, of the kind this study has discussed, but also through consultation of the GAFAM by the U.S. administration.

As an example, during the summer of 2018, the U.S. Department of Commerce was reported to have "been huddling" with Facebook and Google, as well as with internet service providers and consumer advocates, to work on a data privacy proposal.[316] In a sense such consulting is necessary given the lack of technical expertise of the lawmakers, as was evident in 2018 hearings of GAFAM company executives before Congressional committees,[317] but it may also create what may be called an "accountability paradox," and a conflict of interest situation.

Of the GAFAM, Facebook and Google, as highly dependent on personal data for advertising purposes, would have the most to lose if significant privacy legislation were proposed, and they could be expected to fight this with heavy lobbying.[318] Given their financial clout, their ability to lobby helps create an obstacle to any moves to harmonize data privacy legislation at a notably higher level.[319] However, *laissez-faire* policy and GAFAM and other lobbying are not the only obstacles to harmonization—constitutional law differences also enter into the equation.

C. Differing Constitutional Provisions as an Obstacle: The Google Spain case

The differing constitutional provisions in the United States and in the European Union are an obstacle to harmonization of data privacy law in the sense that it is difficult to reconcile the two systems, as this study will show using the case of *Google Spain* to illustrate the difference. This situation arises because of what privacy lawyer Eduardo Ustaran calls a "major philosophical difference between the two jurisdictions," where data protection is a fundamental right in the European Union, but not in the United States,[320] and

315. *See* Meyer, *supra* note 306 (closing the article with the words: "Prepare for a new privacy lobbying battle.").

316. Romm, *supra* note 267 ("[T]he Commerce Department has been huddling with representatives of tech giants such as Facebook and Google Internet providers including AT&T and Comcast and consumer advocates according to four people familiar with the matter but not authorized to speak on the record.").

317. *See, e.g.*, Dylan Byers, *Senate Fails Its Zuckerberg Test*, CNN BUSINESS (Apr. 11, 2018, 4:21 AM), https://money.cnn.com/2018/04/10/technology/senate-mark-zuckerberg-testimony/index.html (reporting that "most of the senators who asked [Mark Zuckerberg] questions had no clue how Facebook worked, what the solutions to its problems are, or even what they were trying to achieve by calling its CEO to testify, other than getting some good soundbites in. What the first day of the Zuckerberg hearings made clear is that many American lawmakers are illiterate when it comes to 21st century technology.").

318. *See* Celia Kang, *Tech Industry Pursues a Federal Privacy Law, on Its Own Terms*, N.Y. TIMES (Aug. 26, 2018), https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html (explaining the aggressive lobbying practices of Facebook, Google, IBM, and Microsoft).

319. *See id*. ("It's clear that the strategy here is to neuter California for something much weaker on the federal level.").

320. Meyer, *supra* note 306.

Rustad and Kulevska describe in a more catchy way as, "Americans are from Mars and Europeans are from Venus when it comes to data privacy and the right to be forgotten."[321] Furthermore, not only does the very broad view of the freedom of speech in the United States—especially with the Supreme Court in *Citizens United* holding that corporations enjoy this right in the context of electoral politics[322]—create a barrier between varying rights on both sides of the Atlantic, it also loops back into the lobbying obstacle discussed in Part II.B, allowing for a greater leeway for corporate political action that could be used to brake any moves toward harmonization. Moreover, Professor Lee Bygrave points to the use of the First Amendment as basis for court challenge of data privacy legislation, pointing to the example of a successful attack on a Vermont law limiting use of pharmacy records for marketing purposes in *Sorrell v. IMS Health, Inc.*[323]

The U.S. Constitution does not mention a right to privacy,[324] much less a specific right to data privacy. Half a century ago, an American scholar debated whether it made sense to adopt a Constitutional amendment to set out a new fundamental right to privacy and thus "provide the basis for direct federal regulation of state police practices and evidentiary procedures and of key private invasions of privacy," which he deemed an "unprofitable and unwise diversion" for many reasons, including that this kind of proposal would likely be opposed by conservatives and liberals alike, preferring development of the law through judicial interpretation and through the development of laws and regulations.[325] However, by contrast to the right of privacy (to the extent that it exists), freedom of speech is enshrined in the First Amendment of the U.S. Constitution.[326] Court interpretation of this freedom has yielded a jurisprudence that is "the most speech protective of any nation on Earth, now or throughout history."[327]

---

321. Rustad & Kulevska, *supra* note 267, at 355.

322. *See, e.g.*, WINKLER, *supra* note 219, at 222. It should be pointed out, however, that corporate donations to political candidates trail those of unions and individuals post-*Citizens United*. Floyd Abrams, *Citizens United: Predictions and Reality*, THE FREE SPEECH CENTURY 93 (Lee C. Bollinger & Geoffrey R. Stone, eds., 2019) ("Nor did we anticipate that labor unions would outspend business corporations in the aftermath of *Citizens United*.").

323. *See* BYGRAVE, *supra* note 21, at 111 ("Even if legislation gets enacted, it will often face challenge in the courts, the litigation typically centering on putative infringement of the First Amendment to the Bill of Rights in the US Constitution. An example is Sorrell v IMS Health, Inc. in which the US Supreme Court overturned a Vermont statute restricting marketeers' use of pharmacy records, on the grounds that the law unduly violated free speech." (citations omitted)).

324. *See, e.g.*, SOLOVE & SCHWARTZ, *supra* note 37, at 35 ("Although the United States Constitution does not specifically mention privacy, it has a number of provisions that protect privacy, and it has been interpreted as providing a right to privacy"); *see also*, ELLEN ALDERMAN & CAROLINE KENNEDY, THE RIGHT TO PRIVACY xiii (1995) ("The word "privacy" does not appear in the United States Constitution. Yet ask anyone and they will tell you that they have a fundamental right to privacy"); MCGEVERAN, *supra* note 47, at 3, ("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").

325. ALAN WESTIN, PRIVACY AND FREEDOM 442–43 (Ig Pub. ed., 2015) (1967).

326. U.S. CONST. amend. I. ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . .").

327. Lee C. Bollinger & Geoffrey R. Stone, *Dialogue*, THE FREE SPEECH CENTURY 1 (Lee C. Bollinger & Geoffrey R. Stone, eds., 2019) (the citation is from Bollinger's voice in the dialogue).

Contrary to the situation in the United States, the right to privacy has been an important part of European constitutional-level law for years. The European Convention on the Protection of Human Rights and Fundamental Freedoms, also known as the European Convention on Human Rights (ECHR),[328] which dates from 1950 and is legally binding on member states of the Council of Europe (including the EU member states), provides a right to respect for private and family life in its Article 8.[329] The European Court of Human Rights, which handles cases under the ECHR, takes a "dynamic and evolutive" view of the ECHR, avoiding a too narrow view of "private life" and allowing for a right to privacy while people are in public.[330] This has been labeled a "living instrument doctrine," which has been contrasted with the doctrine of originalism when applied to the U.S. Constitution.[331] While the right to privacy contained in Article 8 of the ECHR covers what might be called "informational privacy," and thereby significantly overlaps with the EU right to data protection, the two are considered to be distinct, with the latter extending to more data processing activities, and granting more control over personal data to data subjects than the former, including through rights granted to data subjects.[332] Indeed, data protection has been described as being broader than the right to respect for private life, and its application is dependent only on a finding that personal data exist and are processed, with no requirement of proof of an "infringement on private life" in order to apply,[333] once the scope requirements of relevant legislation are met.

Data protection legislation in EU member states dates back to the 1970s and was formalized on an EU level in the 1995 Directive, and later in the GDPR. Furthermore, a later instrument, the Charter of Fundamental Rights of the European Union (the Charter),[334] not only provides for a right to privacy,[335] it also enshrines the protection of personal data as a fundamental right, providing as follows:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access

328. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 221 [hereinafter ECHR].

329. *Id*. art. 8, at 230.

330. Stefan Kulk & Frederik Zuiderveen Borgesius, *Privacy, Freedom of Expression, and the Right to Be Forgotten in Europe, in* The Cambridge Handbook of Consumer Privacy 302 (Evan Selinger et al., eds., 2018).

331. *Id.* at 303.

332. *See* ORLA LYNSKEY, THE FOUNDATIONS OF EU DATA PROTECTION LAW 11 (2015) (distinguishing data processing and data protection); *see also* HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 75, at 19 (describing data protection as "a distinct value that is not subsumed by the right to respect for private life.")

333. *See* HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 75, at 20 (commenting that, "The right to data protection comes into play whenever personal data are processed"). For example, an employer recording employee names and salary may not interfere with private life, however the recording is a processing and the names and salary are personal data, and so data protection rules apply to the employer.

334. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1.

335. *Id*. art. 7, at 10.

> to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[336]

The right to data protection was raised to a higher level as one of the fundamental rights, which are considered as inalienable rights based on grounds of human dignity,[337] including it among protected freedoms alongside the freedom of expression and information.[338] The Treaty of Lisbon[339] changed things, modifying the structure of EU protection of fundamental rights and adding protections of personal data directly into the recast Treaty establishing the European Community (Treaty of Rome)[340]—now known as the Treaty on the Functioning of the European Union (TFEU).[341] Furthermore, an amended version of the Charter[342] was made legally binding in the European Union through the Treaty of Lisbon, which allowed for this in an amended version of the Treaty on European Union.[343]

The Charter is addressed to EU institutions, bodies, offices, and agencies when they are implementing EU law[344] (such as the 1995 Directive or, now, the GDPR), and its inclusion of data protection as a fundamental right and the modifications brought by the Treaty of Lisbon have been accompanied by a show of enthusiasm for this right and the right of privacy by the Court of Justice of the European Union (ECJ).[345] However, fundamental rights under the Charter, as amended, are not absolute, as that instrument provides that there may be limitations on its rights and freedoms, but such limitations:

> must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives

336. *Id*. art. 8, at 10.

337. LYNSKEY, *supra* note 332, at 241.

338. Charter of Fundamental Rights of the European Union, *supra* note 334, art. 11.

339. Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, Dec. 13, 2007, 2007 O.J. (C 306) 1 [hereinafter Treaty of Lisbon].

340. FUSTER, *supra* note 43, at 230.

341. Consolidated Version of the Treaty on the Functioning of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) 16, 47 [hereinafter TFEU]. Article 16(1) of the TFEU now provides "Everyone has the right to the protection of personal data concerning them."

342. Charter of Fundamental Rights of the European Union, *supra* note 334, art. 1.

343. *See* Consolidated Version of the Treaty on European Union, Oct. 26, 2012, 2012 O.J. (C 326) 1, 19 (establishing the legal value of the treaty); Treaty of Lisbon, *supra* note 339, art. 6. The Treaty on European Union, as amended by the Treaty of Lisbon, provides in its Article 6(1) that, "The Union recognizes the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties."; *see* Ottavio Marzocchi, *The Protection of Fundamental Rights in the EU*, at 3 (Oct. 2018), http://www.europarl.europa.eu/factsheets/en/sheet/146/the-charter-of-fundamental-rights (describing the charter becoming binding law). The Charter thus came into direct effect, "becoming a binding source of primary law," in the European Union; FUSTER, *supra* note 43, at 231; *see* HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 75, at 28 (describing the Charter prior to the change as a "political document," and after, legally binding).

344. *See* Charter of Fundamental Rights of the European Union, *supra* note 334, art. 51 (describing what the Charter is designed to be addressed to).

345. *See* LYNSKEY, *supra* note 332, at 63 (discussing the enthusiasm by the Court of Justice of the European Union for the right of privacy).

> of general interest recognised by the Union or the need to protect the rights and freedoms of others.[346]

Thus, where there is a conflict between the fundamental right to data protection and the rights and freedoms of others, the ECJ has stated that there must be a balancing exercise with those other rights or freedoms.[347] Furthermore, the GDPR provides that "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression,"[348] and exemptions or derogations from certain of the provisions of the GDPR are to be provided for by member states in connection with such processing.[349] In addition, personal data in official documents held in connection with a public interest task "may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data" under the GDPR.[350] However, protections for personal data are still taken into account in the balancing or reconciling of rights or freedoms that may come into conflict.

While freedom of expression and information is a fundamental right in the European Union,[351] it is likewise not an absolute right. Thus, as an example, France is subject to the ECHR and to the Charter, but it still may impose certain restrictions on the freedom of expression, such as the part of its media law prohibiting hate speech intended to "provoke discrimination, hate, or violence towards a person or a group of people because of their origin or because they belong or do not belong to a certain ethnic group, nation, race, or religion."[352] A case involving the French media law was the basis for a dispute with Yahoo over the sale of Nazi memorabilia online (which was allowed under freedom of speech in the United States, but not in France), which resulted in Yahoo first using geo-blocking to avoid such sale in France, and then changing its policy to

346. *See* Charter of Fundamental Rights of the European Union, *supra* note 334, art. 52(1) (discussing the limitations to the right of freedom and other fundamental rights set out by the Charter).

347. HANDBOOK ON EUROPEAN DATA PROTECTION LAW, *supra* note 75, at 53.

348. GDPR, *supra* note 16, at art. 85(1).

349. *Id.* art. 85(2).

350. *Id.* art. 86.

351. Freedom of expression is also protected under the ECHR. *See* ECHR, *supra* note 328, art. 10(1) ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."); *see* Charter of Fundamental Rights of the European Union, *supra* note 334, art. 11(1), 10(2) ("Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."). However, such freedom may be subject to restrictions. "The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary."

352. *See* Andrew Weber, *FALQs: Freedom of Speech in France*, IN CUSTODIA LEGIS (Mar. 27, 2015), https://blogs.loc.gov/law/2015/03/falqs-freedom-of-speech-in-france/ ("The French Constitution protects freedom of expression, but not to the same extent as the First Amendment does under U.S. law.").

block such sales worldwide.[353] However, more relevant to our discussion of data privacy is a case illustrating the importance of the differing constitutional provisions in the United States and the European Union–the ECJ *Google Spain* case.[354]

A Spaniard named Mario Costeja González filed a complaint with the *Agencia Española de Protección de Datos* (AEPD)—the Spanish independent administrative authority responsible at the time for monitoring application of the 1995 Directive (and now of the GDPR).[355] The complaint was against, inter alia, Google Spain SL (Google Spain) and Google Inc., applying to have them withdraw from their index personal data concerning him and preventing future access to such data.[356] The personal data was found in pages from the Catalan newspaper, *La Vanguardia*, searchable on the Internet through Google and providing publicity for a real-estate auction for the recovery of social security debts.[357] The AEPD had rejected Mr. Costeja González's request for taking down the newspaper's pages but upheld the request for delisting such pages from Google's search engine results when Costeja's name was searched.[358]

Google appealed the decision to Spain's National High Court, which referred certain questions on the 1995 Directive to the ECJ for resolution.[359] In the case where the legitimate basis for the collection of the personal data was either that processing is necessary for the performance of a task carried out in the public interest, in the exercise of official authority, or necessary for the purposes of the legitimate interests pursued by the controller, the ECJ held that a data subject had a right to object to processing under the 1995 Directive "on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[360] Where there was a right to information for Internet users, a balancing of interests would be made of that right (the freedom of expression and information), and the data subject's right to protection of his personal data and his private life, where one criterion that would tip the balance in the favor of not delisting might have been if the data subject was a public figure, in which event there is a greater interest of the public in access to information.[361] There being no preponderant right to the public to information here (although this was left for the referring court to decide) and the

353. *See* Daskal, *supra* note 205, at 216 (referring to the 2000 decision in a case brought by La Ligue Contre le Racisme et l'Antisémitisme (L.I.C.R.A.) and L'Union des Etudiants Juifs de France (U.E.J.F.) against Yahoo).

354. Case C-131/12 Judgment of the Court (Grand Chamber). *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, 3–5 (2014) (discussing in further detail about a complaint filed by a Spanish citizen about Google's index of his personal data). While the Google Spain case pre-dates the GDPR, the GDPR explicitly includes a right to erasure/right to be forgotten; *see generally* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.L.I. CLJEU 13.05.2014) (holding that Google search results could be taken down).

355. Case C-131/12, *supra* note 354, ¶ 2.

356. *Id.*

357. *See id.* at ¶ 14 (describing the facts of the case).

358. *Id.* at ¶ 15–17.

359. *Id.* at ¶ 18–20.

360. *Id.* at ¶ 76.

361. *Id.* at ¶ 81.

auction sale having occurred years earlier, the ECJ found that, in connection with links to the *La Vanguardia* web pages, "the data subject may…require those links to be removed from the list of results."[362]

This case showed the balancing of two fundamental rights under EU law—the freedom of speech (freedom of expression and information) and the right to protection of personal data, in this instance, the freedom of speech lost out. It also showed the first judicial recognition of a form of the right to be forgotten—the right to delisting[363]—a right that has now been made explicit in the GDPR as the right to erasure ("right to be forgotten").[364] As may be expected, because of the importance of the freedom of speech in the United States, the Google Spain case—and the right to be forgotten—created much interest and comment.[365] It has been noted that this right is "undeveloped" in the United States because of the freedom of speech.[366] According to an academic and a practitioner, such collision between the rights of privacy and speech has not been dealt with to the same extent in the United States as in Europe, but free speech would likely still prevail.[367] Another commentator considers that there are many obstacles to the adoption of the EU right to be forgotten into the United States, citing many observers who would completely discount the possibility because of the overwhelming weight of the First Amendment when balancing with other rights.[368] Other sources gauge the possibility of importing the right to be

362. *Id*. at ¶ 98 ("in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information, a matter which is, however, for the referring court to establish").

363. *See generally*, Gregory Voss & Céline Castets-Renard, *Proposal for an International Taxonomy on the Various Forms of the "Right to Be Forgotten": A Study on the Convergence of Norms*, 14 COLO. TECH. L. J. 281 (2016) (discussing the various forms of the right to be forgotten, generally, and of the Google Spain case).

364. GDPR *supra* note 16, art. 17. One U.S. academic predicted cataclysmic results if the right was to be adopted in the GDPR; *see* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88 (2012) ("[I]t could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet.").

365. *See* Giancarlo F. Frosio, *The Right to Be Forgotten: Much Ado About Nothing*, 15 COLO. TECH. L. J. 307, 311 (2017) ("The recognition by the European Union of a right to be forgotten has ignited disgruntled reactions from legal scholars in the United States and elsewhere. Skeptics argue that the right to be forgotten would endanger freedom of expression and access to information . . . ."); *see also* Voss & Castets-Renard , *supra* note 363, at 286 ("Ever since the Google Spain ruling of the Court of Justice of the European Union ("CJEU") on May 13, 2014, in which a form of the "right to be forgotten" has been at the heart of legal debate in the data protection/privacy sphere . . . .").

366. Rustad & Kulevska, *supra* note 267, at 379 ("Unlike in Europe, the right to be forgotten is undeveloped in the United States in large part because of the hegemony of the First Amendment.").

367. *See* Micheal J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 46 (2017) ("The full collision of competing rights of privacy and speech at the core of the right to be forgotten has not been addressed either in the legal or policy spheres in the United States to the extent it has in Europe. And, for now at least, free speech (and the associated right to know) would likely still prevail over competing privacy rights such as those which are the basis of the right to be forgotten.").

368. *See* MEG LETA JONES, CTRL + Z: THE RIGHT TO BE FORGOTTEN 137 (2016) (describing reasons other than the First Amendment why "the EU version of a right to be forgotten will not be transported into the U.S.," including different weighting of the public interest, because of reliance on intermediary liability, and because of the significance of its scope in limiting access to content); ZUBOFF, *supra* note 184, at 60 ("When the Court of Justice's decision was announced, the "smart money" said that it could never happen in the US, where the internet companies typically seek cover behind the First Amendment as justification for their "permissionless innovation." Some technology observers called the ruling "nuts." Google's leaders sneered at the decision. Reporters characterized Google cofounder Sergey Brin as "joking" and "dismissive.").

forgotten to the United States generally come to similar conclusions.[369] One commentator considers that the First Amendment is a more significant obstacle to the adoption of a right to be forgotten than Silicon Valley (in this study's language, GAFAM) lobbying.[370]

The difference between the constitutional provisions of the United States—where the freedom of speech has what one author calls "firstness,"[371] and privacy is not mentioned—and that of the European Union where privacy (in the ECHR and in the Charter), and the protection of personal data (in the Charter) are placed on the same pedestal with the freedom of expression and information[372] means that it would be very difficult (if not impossible) to harmonize data privacy law between the two partners fully, in a way that would, for example, recognize the right to be forgotten in the United States.[373] Furthermore, the First Amendment tradition has been used to shield data processing and commercial communication from regulation,[374] in the sense of the *laissez-faire* policy described in Section A. This "constitutionalizing" has come through lobbying, trade association, and think tank activity,[375] similar to that discussed in Section B. Indeed, in another context, the First Amendment has been described as "a powerful deregulatory engine."[376] Such statement could also be applied to the area of data privacy in the United States. But, does this, and all the foregoing obstacles to data privacy harmonization from previous sections of this part of the study mean that we should despair?

---

369. *See, e.g.*, Paul J. Watanbe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L. REV. 1111, 1133–1134 (2017)("Instead of providing a unified exportation of the right to be forgotten across the Atlantic, the [GDPR] leaves free expression exceptions to the privacy interest fragmented at the national level."); *see also* Ashley Stenning, *Gone but Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impact of Data Breaches*, 18 SAN DIEGO INT'L L. J. 129, 152–53 (2016) ("[T]he argument that search-engine results are speech and thus protected under the First Amendment from government regulation still stands, which may pose a hurdle in applying the right to be forgotten to include search engines.").

370. *See* John W. Dowdell, *An American Right to Be Forgotten*, 52 TULSA L. REV. 311, 333 (2017) (describing studies that show that the perception is that U.S. law is not keeping up with technology).

371. *See* Albie Sachs, *Reflections on the Firstness of the First Amendment in the United States* in THE FREE SPEECH CENTURY 179 (Lee C. Bollinger & Geoffrey R. Stone, eds., 2019) ("American judges . . . . centered their Constitution on the notion of free speech . . . .").

372. Watanbe, *supra* note 369, at 1115 ("Rights prioritization across the Atlantic is a study of contrast: the United States favors free expression over privacy, and the European Union balances privacy and free expression as coequal fundamental rights.").

373. *See* Edward J. George, *The Pursuit of Happiness in the Digital Age: Using Bankruptcy and Copyright Law as a Blueprint for Implementing the Right to Be Forgotten in the U.S.*, 106 GEO. L. J. 905, 915 (2018) ("[M]ost American commentators have criticized the right to be forgotten and have deemed it completely foreign to American laws and values. The criticisms of the right derive from two American bedrocks: freedom of speech and the right to know."); MCGEVERAN, *supra* note 47, at 297 ("Removing links posted by a private company restricts that company's choices of what content to highlight and it also interferes with the public's ability to find certain information. Such legal requirements may violate current interpretations of the First Amendment.").

374. *See* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. Rev. 133, 162 (2017) ("For some time now, a campaign has been underway to insulate all forms of commercial information processing and direct-to-consumer communications from regulatory oversight on first amendment grounds.").

375. *See id*. at 163 (describing how many companies are participating in data commercialization).

376. *See* Amanda Shanor, *The New Lochner*, 2016 WIS. L. REV. 133, 134 (2016) ("[T]he First Amendment has emerged as a powerful deregulatory engine . . . . This article identifies this important development as a growing constitutional conflict between the First Amendment and the modern administrative state . . . .").

III. CORPORATE ACTION AND HOPES FOR GLOBAL HARMONIZATION IN CONTEXT

Clearly, there are obstacles to data privacy law harmonization, however, is there room for optimism and hope for harmonization? This part briefly addresses corporate action in protecting privacy (Section A), before discussing hopes for harmonization (Section B), and tempering such hopes with an analysis of political and other realities (Section C).

A. Corporate Action

One open point is that, through adopting practices inspired by EU legislation, will the action of tech companies lead to a *de facto* harmonization of practices between companies in the European Union and the United States, without the need for new laws? U.S. multinational companies may "find it convenient" to comply with the higher EU standard for all their customers, making such standard and its rules "de facto practices" in the United States.[377] This may be a strategic choice for companies.[378]

Shortly before the date when the GDPR was to apply, Microsoft announced that it would provide its customers worldwide the same data subject rights that it was required to provide its customers in the European Union under the GDPR.[379] While certainly laudable, this unilateral move is not the equivalent of the adoption of legislation, and only binds one company—Microsoft.[380] Contrast this with the action of Facebook. Previously, Facebook used its Irish subsidiary for the accounts of all its users outside of North America.[381] However, in 2018, Facebook changed its privacy policy to limit the coverage of its customers by its Irish subsidiary to those within the European Union, thus excluding those in Asia, Latin America, and Africa from the protections of the GDPR and the oversight of the Irish data protection agency.[382] Where legislation would have treated both Microsoft and Facebook users in the same way, there is now divergence in privacy treatment, depending on whether you are a customer of Microsoft or Facebook.

---

377. CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 310 (2016).

378. *Compare* Voss & Houser, *supra* note 24, at 336–40, *with* Jordan M. Blanke, *Top Ten Reasons to Be Optimistic About Privacy*, 55 IDAHO L. REV. 281, 306 (2019) (although Blanke recognizes that some aspects of the GDPR may be incorporated by companies, he comments that, "it will be surprising if many companies adopt all of the GDPR," given its "far-reaching requirements").

379. *See* Julie Brill, *Microsoft's Commitment to GDPR, Privacy and Putting Customers in Control of Their Own Data*, MICROSOFT ON THE ISSUES (May 21, 2018), https://blogs.microsoft.com/on-the-issues/2018/05/21/microsofts-commitment-to-gdpr-privacy-and-putting-customers-in-control-of-their-own-data/ (describing how Microsoft would respond to GDPR).

380. *See id.* (describing how Microsoft's commitment to respecting its user's privacy).

381. *See* Mark Scott & Nancy Scola, *Facebook Won't Extend EU Privacy Rules Globally, No Matter What Zuckerberg Says*, POLITICO (Apr. 19, 2018), https://www.politico.eu/article/facebook-europe-privacy-data-protection-mark-zuckerberg-gdpr-general-data-protection-regulation-eu-european-union/ (describing how all of Facebook's users outside of North America were overseen by Irish regulators).

382. *Id.* ("GDPR, will remain off-limits to Facebook users outside the 28-member bloc . . . . under proposed changes, these non-EU users would now have a legal contract with Facebook's U.S. entity, meaning that they would fall under America's privacy standards that are perceived by many privacy campaigners as not as rigorous compared to Europe's upcoming privacy legislation.").

At the fortieth edition of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) held in Brussels, Belgium, in October 2018, Apple CEO Tim Cook called for a U.S. federal privacy law to equalize to the GDPR.[383] However, Apple is less dependent on the use of personal information than Facebook or Google, whose CEOs "heralded the advent of privacy legislation, though in less explicit terms," speaking by video, Google's CEO Sundar Pichai said that his company "is offering its users a greater say over what data the company collects," adding that it "is now advocating for comprehensive privacy principles across its digital services."[384] However, this corporate action is similar to the concept of self-regulation and *soft law*, and as it is voluntary unilateral action, there is no guarantee of either its scope or its continuance. In addition, soft law, even when adopted generally, (that is if an entire sector agreed to it, perhaps through a trade association, and not just through the voluntary action of one firm) may evidence a tension between self-interest and the greater interest of the public and has many weak points, such as not providing a certain clear and reliable framework, not including an element of constraint through the possibility of enforcement, and generally tending toward a "race to the bottom" in policy[385]—all disadvantages to counterbalance claims of advantages from flexibility. Furthermore, empirical evidence has shown that in one area—the use of web trackers mostly to collect data for advertising purposes—one data-privacy-invasive practice has increased in the United States since the application of the GDPR, while the same practice has decreased in the European Union,[386] contrasting—with respect to this specific criterion—the effectiveness of hard law in the European Union against that of self-regulation in the United States. As Professor Joel Reidenberg pointed out some twenty years ago, U.S. firms can choose to provide better data protection for U.S. citizens in order to have harmonization of practices, or choose to treat foreigners better than U.S. citizens.[387]

In summary, while some corporate action may seem promising, the overall picture is less bright, and corporate practices—voluntary corporate action—would not appear to be bringing the United States and the European Union any closer to harmonization.

383. Scott, *supra* note 308.

384. *Id.*

385. *See* ROGER BROWNSWORD & MORAG GOODWIN, LAW AND THE TECHNOLOGIES OF THE TWENTY-FIRST CENTURY: TEXT AND MATERIALS 378 (2012) (listing certain perceived weaknesses of soft law, and also highlighting the potential advantages of soft law in a technological context, such as flexibility); *see also* BÄRBEL DORBECK-JUNG & MARLOES VAN AMEROM, INTERNATIONAL GOVERNANCE AND LAW 133–34 (2008) (describing how a "co-regulatory" strategy may be useful when soft law and self-regulation is preferred).

386. *See* Björn Greif, *Study: Google is the Biggest Beneficiary of the GDPR*, CLIQZ (Oct. 10, 2018), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr (showing that the GDPR became applicable on May 25, 2018 and the European Union showed a decrease in the use of web trackers per page of -3.4%, while the United States showed an increase in the use of trackers by +8.29%).

387. *See* Reidenberg, *supra* note 105, at 780 (stating that "Ironically, American companies' global electronic commerce activities face an heretical choice: either provide better protection for U.S. citizens in order to have a single set of practices for global operations (because foreign laws require fair information practices) or maintain a double standard, treating foreign citizens to better privacy than U.S. citizens.").

B. Hopes for Global Harmonization

In the matter of data privacy, hope for harmonization of legislation among certain academics springs eternal. A decade ago, one academic reported that a, "broad coalition" of companies, including some of the GAFAM, had, "formed in support of a national information privacy law," with potential benefits including that, "it would harmonize the U.S. regulatory approach with that of the European Union (EU), and possibly minimize international regulatory conflicts about privacy."[388] To date, no such law has been adopted by the United States.

Recently certain other academic voices have been raised that express hope for global harmonization, or even the view that there already is harmonization in data privacy law between the United States and the European Union.[389] In one example, Professors Rustad and Koenig point to several areas where the GDPR adopts practices that already exist in the United States: deterrence-based fines, wealth-based punishment, collective redress, and a data subject's, "right to initiate public enforcement." The authors claim that, "the net effect of this European recognition of the benefits of U.S. remedies is a bilateral transatlantic privacy convergence,"[390] however, these practices are only part of the picture. While here and elsewhere certain elements common to American law are noted to have been adopted in the GDPR,[391] much as the FIPPs are at the basis of data privacy principles in the GDPR,[392] what the authors fail to note is that the fact of the adoption of such practices, which are spread throughout the U.S. legal system, do not bring the two trade players' data privacy laws into line. U.S. law remains based on self-regulation,[393] with certain sectoral statutes,[394] but lacks the general coverage of EU law.[395] Data subject rights provided by EU law are not consistently available in the United States, even if many of them have the same FIPPs origins, as Rustad and Koenig remark,[396] and as is discussed in Part I.A.

388. Schwartz, *supra* note 307, at 904 (arguing that it would be problematic for the U.S. to preempt private sector privacy law with comprehensive federal law).

389. *See, e.g.*, Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365 (2013) (describing how American and European laws around privacy and free speech interact).

390. Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 368–69 (2019).

391. *See, e.g.*, W. Gregory Voss, *Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation*, 50 REVUE JURIDIQUE THÉMIS 783, 802 (2016) (discussing the development of the American-influenced concept of accountability in the GDPR).

392. *See supra* Part I.B.2 (highlighting the passing of the GDPR).

393. *See* John Black & Mike Dunne, *Chapter 8: Information Security*, INTERNET LAW FOR THE BUSINESS LAWYER 159, 169 (Juliet M. Moringiello, ed., 2d ed., 2012) (referring to the United States following the model of having "laws based on a self-regulatory/sectoral approach").

394. *See supra* Part I.B.1 (outlining the passing of laws in the United States).

395. *See* Schwartz & Peifer, *supra* note 35, at 136 (stating that, "U.S. law does not protect the individual through an omnibus law. Rather, information privacy law takes the form of a patchwork that includes statutes as well as regulations at both the federal and state level.").

396. Rustad & Koenig, *supra* note 390, at 419.

C. Political (and Other) Realities

It has been reported that, "[B]oth the Trump administration and lawmakers have begun crafting proposals for a national privacy law, setting up a yearslong struggle over the future of Facebook's data-hungry business model."[397] However, that struggle will not just be waged with Facebook,[398] but also with other beneficiaries of cheap personal data, such as Google, and digital advertising trade associations, among others. Furthermore, the result of U.S. tech companies' lobbying efforts may be to help fashion a weaker federal statute, such as to preempt CaCPA without placing too many restrictions on their activity.[399] Finally, if any legislation eventually results, it will likely take years to achieve and likely not resemble the GDPR. Indeed, U.S. Secretary of Commerce Wilbur Ross penned an editorial piece that criticized the GDPR shortly after its application date.[400] Thus, it seems unlikely that the administration to which he belongs would clone that EU legislation.

Moreover, the U.S. political landscape has been littered with remnants of evidence of the good intentions of the executive and legislative branches of government to adopt more comprehensive and protective data privacy legislation. However, such proclamations have been accompanied by a lack of political will[401] in the face of determined lobbying, making them dead letter. This may be what Bennett and Raab were alluding to when they referred to "a flurry of electorally motivated legislative proposals in the American Congress," after the adoption of the 1995 Directive in Europe.[402] Gellman and Dixon also recognize this difficulty. While they acknowledge a harmonization of data privacy rules in many nations worldwide, the United States is not one of these.[403]

---

397. Sheera Frenkel, et al., *Delay, Deny and Deflect: How Facebook's Leaders Fought Through Crisis*, N.Y. TIMES (Nov. 14, 2018), https://nyti.ms/2DlsGPi.

398. The fight with Facebook could be a difficult one. To provide a past example that might give a hint of what is to come, in 2017, Facebook COO Sheryl Sandberg, "embarked on a hard-edged lobbying campaign to discredit the company's critics and push back on the growing chorus of voices calling for Facebook and other big tech companies to be broken up or more tightly regulated." Nicholas Confessore & Matthew Rosenberg, *Sheryl Sandberg Asked for Soros Research, Facebook Acknowledges*, N.Y. TIMES (Nov. 29, 2018), https://nyti.ms/2DUaHjs.

399. *See supra* Part II.B.3 (discussing lobbying as an obstacle to harmonization).

400. *See* Wilbur Ross, *EU Data Privacy Laws are Likely to Create Barriers to Trade*, FIN.TIMES (May 30, 2018), https://www.ft.com/content/9d261f44-6255-11e8-bdd1-cc0534df682c (criticizing the GDPR in an opinion piece, based on compliance costs, what he calls "unclear legal obligations," and various aspects that he describes as "barriers" (for trade, law enforcement, etc.). Essentially, Secretary Ross, while giving lip service to protecting personal data online, argues for a liberal view of data trade, saying, "We believe that data sharing rules must respect privacy and protect our shared interests of maintaining public safety and the easy functioning of the internet, while also taking into account the regulatory, scientific, and commercial needs of all our countries").

401. One example might be the three-year time period that it took for the Obama White House to release a draft consumer privacy "bill of rights" bill after having issued a White Paper (which failed to result in legislation). *See* Gellman & Dixon, *supra* note 156, at 74–75 (the authors comment the following about the period from 2015–2016 during the 114th Congress: "While many privacy bills and legislative proposals continue to circulate, there is scant political consensus about what to do. Even a more effective Congress rarely produces results in the absence of consensus."); *see also* Romm, *supra* note 267 (remarking on the three-year time period and stating that "Congress never even came close to legislating").

402. BENNETT & RAAB, *supra* note 20, at 117.

403. Gellman and Dixon state that: "Our empirical study of global privacy standards demonstrates that nations around the world are bringing up-to-date their data privacy laws to be harmonized with the EU's

Furthermore, the United States has been seen as playing a negative role in data privacy internationally, seeking to block elements of data privacy law that impose cross-border restrictions on data exported to the United States.[404]

Political will is necessary to make the changes required to allow for transatlantic harmonization of data privacy law. In the current American administration, this study argues that will is lacking.[405] Furthermore, it may be contended that such was the case in the past. As Paul Ohm pointed out in 2015, "The drumbeat for reform has only quickened and grown louder since the Snowden leaks. Yet nothing ever changes."[406] Moreover, Ohm contends, the United States is unlikely to adopt similar privacy protections to the 1995 Directive (of which the GDPR is an evolution) because there is no consensus that the problem is serious enough to warrant such measures.[407] Dilution of legislation by lobbying has also been seen as one of a few factors limiting the potential for effective U.S. privacy law reform,[408] as has already been argued in this study.[409] Recently, although a former Obama administration acting Commerce secretary indicated that lawmakers had the political will to adopt legislation, it was reported that, "Momentum in both chambers has dissipated" for a federal privacy bill.[410]

While some American academics seek compromise between the systems of the two trade players,[411] this viewpoint ignores the reality that the GDPR should be with us for many years. As then-European Data Protection Supervisor Giovanni Buttarelli said in 2016, half a year after the entry into force of the GDPR (but a year and a half before it became applicable), "Make no mistake: the GDPR is here to stay for a long, long time."[412] Viviane Reding, the former European Commissioner for Justice who proposed the GDPR, commented that,

---

comprehensive data protection regime. The U.S. is a possible holdout because of the Trump Administration's recent attempt to blunt the impact of this increasingly adopted EU privacy law." *See* Gellman & Dixon, *supra* note 156.

404. *See, e.g.*, GREENLEAF, *supra* note 23, at 549 (commenting that, "As in the past three decades, it seems that for the near future, the key element of US personal information policy will be negative: to prevent the constantly increasing number of countries that do have data privacy laws from applying those laws to prevent exports of personal data to the USA.").

405. This view coincides with the Trump adminstration's desire for preemptive federal data privacy legislation, mentioned *supra* note 5, which would presumably weaken the protections offered by state legislation such as the CaCPA.

406. Ohm, *supra* note 27, at 1128 (And, it might be added, this is true even though there have been proposals of "sweeping privacy reform.").

407. *See id*. at 1129–30 ("[W]e lack widespread agreement that the general problem of privacy invasion is significant enough to justify such a sweeping approach.").

408. *See* Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. ON REG. 667, 693 (taking the position that it is unlikely that Congress will create general privacy rules to benefit consumers, and adding that, "New Congressional enactments would face familiar undertows in the form of swift obsolescence, dilution by industry lobbying, or the well-documented tendency to target specific technologies" (citation omitted)).

409. *See supra* Part II.B.

410. *See* Daniel R. Stoller, *Lawmakers Are Far Apart on Privacy Bill Despite Pressure to Act*, BLOOMBERG LAW (Aug. 16, 2019, 3:45 AM), https://news.bloomberglaw.com/privacy-and-data-security/lawmakers-are-far-apart-on-privacy-bill-despite-pressure-to-act (reporting on the difficulty of passing a new act).

411. *See supra* Part II.B.

412. Giovanni Buttarelli, European Data Protection Supervisor, *Keynote speech to the IAPP Europe Data Protection Congress 2016* (Nov. 9, 2016), https://edps.europa.eu/sites/edp/files/publication/16-11-09_iapp_speech_gb_en.pdf.

"This regulation needs to stand for 30 years…."[413] Its predecessor, the 1995 Directive, survived some twenty-three years until repealed by the GDPR.[414] Indeed, the future in Europe may involve combining enforcement of data protection laws and competition laws,[415] rather than any change to the GDPR. Moreover, when the GDPR was being debated, the provisions of the then-existing 1995 Directive were seen as a "red line" below which EU parliamentary negotiators would not go,[416] and it is foreseeable that the current GDPR provisions would likewise constitute a red line for any—distant—future negotiations for its replacement. While debates about an ideal data privacy law may be of great intellectual interest, given geopolitical realities, such debates are moot in the context of this study.

Those geopolitical realities include the reality that EU data privacy law is becoming (or has become) the international standard,[417] with strong incentives for other countries to imitate its standard in order to have their data protection deemed "adequate" so as to allow personal data transfer from rich Western Europe, and an easier-to-adopt model than the sectoral one in the United States.[418] This is occurring through, in part, trade negotiations, and potential trade rules on data.[419] As an evidence, if harmonization is to occur, it should involve a movement of the United States towards the EU standard, with a goal of obtaining a Commission adequacy decision.

413. *See* Rosen, *supra* note 364, at 92 (citation omitted) (discussing the enforcement of the European Union law).

414. The 1995 Directive was repealed with effect from May 25, 2018. GDPR, *supra* note 16, at art. 94(1).

415. *See, e.g.*, Natasha Lomas, *Europe is Drawing Fresh Battle Lines Around the Ethics of Big Data*, TECHCRUNCH (Oct. 3, 2018), https://techcrunch.com/2018/10/03/europe-is-drawing-fresh-battle-lines-around-the-ethics-of-big-data/ (reporting that Buttarelli "says he will publish a manifesto for a next-generation framework that envisages active collaboration between Europe's privacy overseers and antitrust regulators").

416. *See* Jennifer Baker, *EU Threesome Promises Good Times for Data Protection Reform*, THE REGISTER (Jun. 24, 2015 15:56), https://www.theregister.co.uk/2015/06/24/things_can_only_get_better_for_eu_data_protection/ (discussing the EU Parliament's LIBE Committee Claude Moraes, stating "any provisions [on protecting personal data] that go below the current 1995 directive would be a red line.").

417. *See, e.g.*, Adam Satariano, *G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog*, N.Y. TIMES (May 24, 2018), https://nyti.ms/2Lq0rAC (discussing the likelihood of nations like Brazil, South Korea and Japan following the EU's lead on data protection legislation). With respect to nations in Asia, *see* GREENLEAF, *supra* note 23, at 12 (noting the impact of the 1995 Directive on Asian data privacy laws); Schwartz & Peifer, *supra* note 35, at 122 (stating that, "EU data protection law has been stunningly influential; most of the rest of the world follows it"); *see also* Voss & Castets-Renard, *supra* note 363, at 314–24 (showing the influence of the 1995 Directive on recent legislation in Africa, Asia, and Latin America); MCGEVERAN, *supra* note 47, at 300 ("Most nations outside the US that have adopted significant privacy laws have gravitated toward comprehensive data protection statutes similar to the EU model.").

418. *See* Voss & Castets-Renard, *supra* note 363, at 303–04 (noting the effect of the 1995 Directive's restriction on cross-border transfers of personal data to countries not deemed to have "adequate" data protection on encouraging the adoption of similar legislation); *see, e.g.*, HOOFNAGLE, *supra* note 377, at 307 (noting international privacy efforts).

419. *See* Laurens Cerulus & Mark Scott, *Europe Seeks to Lead a New World Order on Data*, POLITICO (June 7, 2019, 7:00 AM), https://www.politico.eu/article/europe-trade-data-protection-privacy/ (last updated June 10, 2019 5:15 AM) ("In its trade negotiations with other countries, the EU has insisted on parallel negotiations over so-called adequacy decision deals, or complex data protection agreements in which European regulators must approve another country's privacy regime before companies can easily transfer data outside of Europe.").

One solution, put forward at the end of 2018 by the Commission in its report issued following the second annual review of the Privacy Shield, is that the United States join Convention 108. The report stated:

> Given the significance of transatlantic data flows, the Commission encourages the U.S. to adopt a comprehensive system of privacy and data protection and to become a Party to the Council of Europe's Convention 108. It is through such comprehensive approach that convergence between our two systems can be achieved in the longer term, which would also strengthen the foundations on which the Privacy Shield framework has been developed.[420]

This would require the United States to adopt legislation in many ways equivalent to that of the GDPR, which might result in the United States being deemed to provide "adequate" protection of personal data.[421] This might thereby avoid the need for a Privacy Shield framework between the European Union and the United States. Nonetheless, the obstacles described in this study could prevent such an action.

However, complete transatlantic harmonization of data privacy law—which would allow companies to benefit from a standardized set of rules with which to comply—is not required in order for the United States to obtain a Commission adequacy decision. In its adequacy referential, the Article 29 Data Protection Working Party highlighted that the standard to be met is "essentially equivalent" protection as set out by the ECJ in its *Schrems* decision.[422] According to the ECJ, the word "adequate" means that "a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order," and that an adequate level of protection requires "the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union… ."[423] Although the means used to ensure an adequate level of protection may vary,[424] there is basic content that must be contained, which is derived from data protection principles that originated in the FIPPs: lawfulness and fairness of processing, purpose

420. *Report from the Commission to the European Parliament and to the Council on the Second Annual Review of the Functioning of the EU-U.S. Privacy Shield*, at 6, COM (2018) 860 final (Dec. 18, 2018), https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

421. However, accession to Convention 108 does not guarantee an adequacy finding. Of the non-EU Council of Europe member states listed in *Chart of Signatures and ratifications of Treaty 108*, *supra* note 73, only Andorra and Switzerland have received an adequacy decision; of the non-Council of Europe countries that have acceded to Convention 108, only Argentina and Uruguay have. *See supra* Part I.A.3 (providing background on Convention 108). For a full list of countries that have benefited from an adequacy decision, see *Adequacy of the Protection of Personal Data in Non-EU Countries*, EUR. COMM'N (last visited on Aug. 24, 2019) https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.

422. Art. 29 Working Party, *Adequacy Referential* (WP 254 rev.01) at 3 (Feb. 6, 2018) ("the objective is not to mirror point by point the European legislation, but to establish the essential – core requirements of that legislation"), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108. The EDPB endorsed the Adequacy Referential. *See* European Data Protection Board, Endorsement 1/2018 at 2 (May 25, 2018), https://edpb.europa.eu/sites/edpb/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

423. 2016 E.C.J. 650, *supra* note 189, at 671.

424. *Id*. at 675.

limitation principle, data quality and proportionality principle, data retention principle (in the GDPR: storage limitation), security and confidentiality principle (in the GDPR: integrity and confidentiality), transparency principle, right of access, rectification, erasure and objection, and restrictions of onward transfers.[425] Among the other requirements for adequacy is having a "competent independent supervisory authority," responsible for monitoring, ensuring and enforcing compliance and also a requirement of accountability on the part of data controllers and processors.[426] Three American scholars have suggested that this authority should be the FTC, although it would need to be freer from political pressure, and have a clearer mandate, among other required changes.[427] The measures they suggest could bring the FTC more in line with European requirements. Furthermore, safeguards should exist with respect to State processing of data in connection national security, for example in the field of surveillance, in order to protect against interference of the fundamental rights of persons whose personal data is transferred from the European Union to the United States.[428]

In summary, U.S. policymakers may aim at greater transatlantic harmonization of data privacy law, in order for companies to reap the benefits of reduced compliance costs, and also may accept a goal of a Commission adequacy decision for any future data privacy legislation, thus seizing the opportunity for greater facility for cross border personal data flows. However, they should keep in mind the obstacles that they will face and work in advance to reduce those obstacles to the extent possible. True bipartisan political will may help to overcome the lobbying obstacle, for example. The differences in constitutional provisions obstacle may be more problematic, however. Although the Adequacy Referential does not specifically mention a "right to be forgotten," it does contain a reference to rights from which such right has been derived: the rights of erasure[429] and objection, which could lead to conflicts with the First Amendment.

In a perfect world, the new American legislation should be omnibus and not sectoral, should go back to origins—incorporating the FIPPs—and should aim at a high level of protection, rather than seeking to establish through preemption a lower standard than those set by states. A real independent supervisory authority should be established in order to ensure true compliance and enforcement of the new rules. As previously noted, three scholars have

425. Adequacy Referential, *supra* note 422, at 5–6.

426. *Id*. at 7–8.

427. *See* Chris Hoofnagle et al., *The FTC Can Rise to the Privacy Challenge, but Not Without Help From Congress*, BROOKINGS (Aug. 8, 2019), https://www.brookings.edu/blog/techtank/2019/08/08/the-ftc-can-rise-to-the-privacy-challenge-but-not-without-help-from-congress/ ("But if the FTC is to be a successful regulator of tech platforms, it needs more resources, more tools, a greater shield from political pressure, and a clear Congressional mandate.").

428. *Id*. at 9 (setting out four essential guarantees in this context: 1. "Processing should be based on clear, precise and accessible rules (legal basis)," 2. "Necessity and proportionality with regards to legitimate objectives pursued need to be demonstrated," 3. "The processing has to be subject to independent oversight," and 4. "Effective remedies need to be available to the individuals").

429. In fact, the corresponding GDPR article is entitled "Right to erasure ('right to be forgotten')." GDPR, *supra* note 16, at art. 17.

suggested that this authority could be the FTC, with several important changes to that institution,[430] although this study considers that it would perhaps be more efficient to create a new independent and dedicated data privacy agency, which is a point for further study. In this way, Americans could potentially benefit from protections for their personal data that are similar to those that American companies must offer EU persons, when they offer goods or services (including free ones) to them, or when such companies receive their data through the Privacy Shield mechanism.[431] Whether all this is possible in the face of the obstacles set out in this study is for the future to tell, although it would now seem difficult to overcome all the hurdles discussed.

CONCLUSION

Data privacy law on both sides of the Atlantic benefits from common origins which crystalized in the setting out of principles known as the FIPPs in the U.S. HEW Report. Based on the FIPPs, influential international data privacy guidelines were produced by the OECD, and the first binding international data privacy convention—Convention 108—was established by the Council of Europe. At that time, the U.S. could have taken the lead on data privacy but chose instead to adopt narrow sectoral legislation instead of the omnibus FIPPs-based legislation adopted in the European Union, to favor self-regulation, and not to create a true independent data privacy supervisory authority.

These last developments led to divergence, where once convergence had existed, causing compliance challenges for companies, which had then to deal with different standards. In addition, the threat of the halting of cross-border data flows from the European Union to the United States raised itself as the latter jurisdiction did not evidence the adequate level of data protection in its legislation that was required by EU legislation.

Harmonization of data privacy law would obviate such difficulties; however this study has identified three major obstacles to full-scale harmonization of data privacy law: *laissez-faire* policy and neoliberalism in the United States (and resulting focus on self-regulation there), the lobbying power of the GAFAM in a conducive U.S. legislative system, and differing constitutional provisions on both sides of the Atlantic, where certain rights classified in Europe as fundamental rights—on the same level as the freedom of expression and information—are not mentioned in the U.S. Constitution, where the freedom of speech is the first of freedoms.

Nonetheless, corporate action in the United States might have given some hope of a *de facto* harmonization of practices (absent a harmonization of laws); however, practices diverged there. Certain academics also expressed hope of

430. Hoofnagle, *supra* note 427.

431. Professor Joel Reidenberg is reported to have said, in connection with the Privacy Shield's predecessor—the Safe Harbor—which was then being negotiated, "The Commerce Department is in essence arguing that the companies will commit to strong privacy protection for EU data when it is processed in the US, but we will not give that level of privacy protection to US citizens at home. That is a very troubling statement." *See* James Glave, *Safe Harbor: No Port in a Storm?*, WIRED (Apr. 28, 1999 04:30 PM), https://www.wired.com/1999/04/safe-harbor-no-port-in-a-storm/.

legal harmonization, however there is no evidence of this today, and political and other realities leave reason to be dubitative about the prospects of harmonization.

While a move to greater harmonization seems possible, true (or even meaningful) harmonization seems unlikely, given the obstacles that have been identified in this study. Perhaps weak federal data privacy legislation may see the light of day in the United States, through lobbying by the GAFAM and other companies to preempt state legislation such as the CaCPA. One way forward toward more significant harmonization would be for the United States to accede to Convention 108, however that would require providing GDPR-like protections to personal data, and given the obstacles defined in this study, this seems unlikely. Achievement of a Commission adequacy decision should be a goal, however this effort would face the obstacles detailed in this study as well. Thus, issues of compliance with differing legal standards and potential barriers to cross-border data transfers are likely to remain.

ANNEX

Summary of Principles from HEW Report and Various Data Privacy Instruments

HEW Report FIPPs	**OECD Guidelines**	**Convention 108**	**GDPR Data Protection Principles**
Data quality: correct or amend; reliability for intended use	Data quality: relevant; accurate, complete and up-to-date	Data quality: adequate, relevant and not excessive; accurate and kept up-to-date	Data quality: accuracy; data minimization; storage limitation
Purpose specification	Purpose specification	Purpose specification	Purpose limitation (subsuming purpose specification & use limitation)
Use limitation	Use limitation	Use limitation	
Security safeguards	Security safeguards	Data security	Integrity and confidentiality
Transparency	Openness	Transparency of processing	Transparency
Rights of the data subject	Individual participation	Rights of the data subject	Rights of the data subject (expanded, particularly to include a right to data portability and a "right to be forgotten")
	Accountability	Additional obligations	Accountability (with new tools such as DPOs and DPIAs)
	Collection limitation	Legitimacy of data processing	Lawfulness and fairness of processing