EU INFLUENCE ON DATA PRIVACY LAWS:

IS THE US APPROACH CONVERGING WITH THE EU MODEL?

EMMANUEL PERNOT-LEPLAY*

INTRODUCTION

Around the world, countries are enacting data protection laws to keep-up with the pace of technological advancements. To address new issues, they must quickly find legal solutions to answer complex problems. Previous studies have shown that these countries tend to look to the European Union's ("EU") laws on personal data protection as a model and import its rules into their domestic legal frameworks.[1] The EU model relies on one comprehensive law to regulate personal data protection issues, providing strong guarantees to data subjects.[2] This external influence is not only due to the credibility that EU laws have built

* Emmanuel Pernot-Leplay is a Ph.D candidate in comparative law at Shanghai Jiao Tong University, Koguan Law School, focusing on data protection and privacy rules in the EU, the U.S. and China. The author would like to thank the editors of the *Colorado Technology Law Journal* for their work and insightful comments.

1. *See infra* Section I.A.
2. *Id.*

over time, but also to the lack of a competing model in the field of privacy.[3]

The U.S. prefers a different approach, which is not as influential as the EU's and likely cannot prevent the EU approach from becoming, de facto, the global norm.[4] In contrast to the EU model, the U.S. regulates the protection of personal information and privacy through several laws with a narrow scope.[5] This approach is now being challenged by data privacy scandals and the rise of the EU's regulatory clout on this issue.[6] Yet, the current state of research mostly focuses on highlighting the differences between approaches on both sides of the Atlantic.

This article shifts this focus and looks at whether the EU model's influence could extend to the U.S. Therefore, the relevant question seeks to understand why the EU's model became so influential, what is the basis for the U.S. divergence, and are there signs of convergence between U.S. and EU laws?

To answer these questions, I first turn to theories on legal transplantation discussed in the comparative law literature. I believe that to understand the drivers of European influence, rather than solely examining the motivations of the recipient country importing the rules it is also necessary to analyze the donor country's rationale for exporting its rules. I then examine the legal basis for the different approaches to data protection. In studying the different philosophies underlying each approach, I expose the rationale for the significant differences between EU and U.S. privacy law. Going further, I examine initiatives in various U.S. states to find significant signs of convergence already underway.

The article first demonstrates how the EU's influence is facilitated by the international context and the lack of competing model, thereby fostering the transplantation of EU rules in foreign countries (Section I.A). Section I.B then explores the drivers behind the EU's desire to spread its data protection model to the rest of the world. The article next analyzes the different philosophies driving the protection of personal data in both countries in order to explain why the U.S. approach is divergent and historically immune to the EU's influence (Section II.A). Finally, the last section considers

3. *Id.*

4. *See* William Alan Reinsch, *Must Third Countries Choose Between EU or U.S. Digital Trade Protection Preferences?*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (July 11, 2018), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/must-third-countries-choose-between-eu-or-us [https://perma.cc/HQF4-BW28] (last visited Jul 13, 2019).

5. Shawn Marie Boyne, *Data Protection in the United States,* 66 AM. J. COMP. L. 299–343 (2018).

6. *See* Reinsch, *supra* note 4.

recent legal developments in the U.S. which demonstrate convergence with EU rules and discusses how the federal government could react to that convergence (Section II.B).

I. THE RATIONALE BEHIND THE EU'S INFLUENCE ON PERSONAL DATA PROTECTION

A. Lack of a Competing Model

Despite a basic and essential need to regulate data protection at the international level due to the of ease of transmitting information between countries, there is not yet a widely adopted international treaty promoting strong data protection. However, several attempts have been made at the international level to outline common principles. In the beginning of the 1980s, the Organization for Economic Co-operation and Development ("OECD") issued its Privacy Guidelines,[7] and the Council of Europe passed Convention 108.[8]

The Privacy Guidelines set forth non-binding fundamental data protection principles (namely collection limitation, data quality, use limitation, purpose specification, data security, transparency, individual participation and accountability)[9] and has recently been updated to strengthen the accountability principle promoted by the EU.[10] These basic principles are considered to be the minimum international standards. Notably, however, they do not require specific protection for sensitive data. This is the result of an early dispute between the EU and the U.S. in which the U.S. contended, contrary to the European view, that the value of data is highly context-specific and not sensitive in itself.[11] Although these principles are often found in data protection laws,[12] the OECD Privacy Guidelines are only a soft law instrument.

7. ORG. FOR ECON. CO-OPERATION & DEVELOPMENT, GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (last updated 2013) [hereinafter *OECD Privacy Guidelines*].

8. Council of Europe, Details of Treaty No. 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Jan. 28, 1981.

9. *OECD Privacy Guidelines*, *supra* note 7, Part 2.

10. OECD *WORK ON PRIVACY,* https://www.oecd.org/sti/ieconomy/privacy.htm [https://perma.cc/LC7C-VLV6] (last visited Sept. 8, 2019).

11. Anneliese Roos, *Core Principles of Data Protection Law*, 39 THE COMP. & INT'L L.J. S. AFR. 102, 121–122 (2006).

12. Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 73 (2012).

By contrast, Convention 108 is an international treaty and is the only legally binding instrument in the field.[13] The Convention mandates that countries adhering to it must pass laws reflecting its principles. Beyond reflecting the OECD Privacy Guidelines, Convention 108 expands data protection; most notably, it does so by requiring data minimization, data breach notification, accountability, and special treatment for sensitive data.[14] The stronger requirements set forth in the Convention have subsequently been included in EU rules.[15] Furthermore, the EU has since increased its level of protection to surpass the protections offered by Convention 108.[16]

Despite its European origin and the fact that all original members to the Convention were European, the Convention may be ratified by any country; recently more and more foreign countries are joining it or considering doing so.[17] This trend spurs hope that Convention 108 has the potential to become the first widely adopted international data protection treaty and some scholars are hopeful that the United Nations may eventually adopt Convention 108.[18]

Thus, the current lack of a truly global treaty on personal data protection leaves the possibility that countries will advance their own, unique approach. The EU took the lead on this issue, and so far, is not challenged by a strong alternative model. As detailed below, because the U.S. does not have a comprehensive national privacy law, its approach is difficult to follow and leaves the EU as the only reference model in the field. This provides an opportunity for the EU to expand its regulatory clout "[i]n the absence of an alternative American model, it seems like the [General Data Protection Regulation ("GDPR")] will rule the data protection

13. Council of Europe, *Modernisation of the Data Protection "Convention 108"* (Jun 24, 2019), https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet [https://perma.cc/KM88-GG6D].

14. *Id.*

15. Greenleaf, *supra* note 12 at 73.

16. Graham Greenleaf, *Renewing Data Protection Convention 108: The CoE's 'GDPR Lite' Initiatives*, 142 PRIVACY LAWS & BUS. INT'L REP. 14–17 (2016).

17. GRAHAM GREENLEAF, CONVENTION 108+ AND THE DATA PROTECTION FRAMEWORK OF THE EU 1 (2018), https://papers.ssrn.com/abstract=3202606 ("Although it originated from the Council of Europe, since 2011 data protection Convention 108 is steadily being 'globalised'. In addition to its 47 European parties, five countries outside Europe are now Parties: Uruguay, Mauritius, Senegal, Tunisia and Cape Verde…Four more countries have had Accession requests accepted, but have not yet completed the accession process: Morocco, Argentina, Mexico, and Burkina Faso. Eleven other countries, or their [data protection authorities], are now Observers on its Consultative Committee"),.

18. GRAHAM GREENLEAF, *The UN Should Adopt Data Protection Convention 108 as a Global Treaty* 1 (2018), https://papers.ssrn.com/abstract=3159846 [https://perma.cc/YV8X-HPB4].

roost."[19] Even China, which was initially closer to the U.S. approach, is now showing signs of convergence with the EU model.[20]

Furthermore, the legal literature demonstrates that EU data protection laws influence both business practices[21] and third countries' laws.[22] On the former, Professor Anu Bradford of Columbia University, articulates that EU rules are successful at shaping foreign companies' practices even when they operate outside the reach of EU law – thereby reinforcing the EU as a regulatory superpower – pursuant to what she calls the *Brussels Effect*.[23] This phenomenon applies to several fields, including data protection.[24]

The latter explains the phenomenon known as legal transplantation where a country imports foreign legal rules in its domestic legal system.[25] In the field of personal data protection, the EU's clout is driven by its first mover advantage, its strong democratic backing, and the transparent functions of its data protection framework. It is also aided by the fact that it is governed by independent supervisory authorities that enforce and promote the rules, as well as publicly communicate their opinions on various issues.

These features make it a convenient reference model for third countries to import rules from, rather than creating their own model at great expense, to both time and money. It corresponds to what Jonathan Miller, a professor of law and expert on legal evolutions in Latin America, calls the "cost-saving transplant" in his seminal article about the motivations behind the transplantation of foreign rules.[26] Using this type of transplant, a

19. *See* Reinsch, *supra* note 4.

20. Emmanuel Pernot, *Protection des données : la Chine en marche vers le modèle européen*, LESECHOS (Jan. 3, 2018), https://www.lesechos.fr/idees-debats/cercle/protection-des-donnees-la-chine-en-marche-vers-le-modele-europeen-129939#Xtor=AD-6000 [https://perma.cc/E5AG-FEHK].

21. *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 23 (2012).

22. *See* Greenleaf, *supra* note 13; Graham Greenleaf, *'European' Data Privacy Standards Implemented in Laws Outside Europe*, 149 PRIVACY L. & BUS. INT'L REP. 21–23 (2017).

23. Bradford, *supra* note 21.

24. Bradford identifies four other fields in addition to privacy: antitrust laws, health protection, environmental protection and food safety. Bradford, *supra* note 21, at 19-32.

25. Most notably introduced by Alan Watson. *See generally* ALAN WATSON, LEGAL TRANSPLANTS: AN APPROACH TO COMPARATIVE LAW (1 ed. 1974).

26. Jonathan M. Miller, *A Typology of Legal Transplants: Using Sociology, Legal History and Argentine Examples to Explain the Transplant Process*, 51 THE AM. J. OF COMP. L. 839, 845–46 (2003). Other types of transplants are the externally-dictated transplant, the legitimacy-generating transplant and the entrepreneurial transplant, which can be a result of the above-mentioned Brussels Effect.

third country implements a solution already established and implemented in a foreign legal system which saves time, investment, and the trial-and-error route of a homegrown legal solution.[27] This implies that both the donor and recipient countries faced similar problems, because the transplanter looks for a foreign rule solving the problem that it faces.[28]

Graham Greenleaf, a professor of law who has undertaken extensive research on privacy laws around the globe, highlights that several elements specific to EU data protection rules are transplanted in third countries' laws.[29] While the number of countries adopting a data protection law following the EU standards is increasing, the sectoral approach favored by the U.S. is losing traction.[30] EU law also contributes to the development of data privacy certifications[31] and has helped to shape laws in French-speaking African countries.[32] In the 2017 update to Greenleaf's research, he shows that the trend demonstrating European data protection influence remains strong.[33] His comparison excludes the U.S. because he considered only countries with a comprehensive data protection law akin to the instrument favored by the EU, whereas the U.S. has laws of limited scope.[34] Despite this divergence in legal structure and the current lack of a nationwide privacy law in the U.S., this article will show that convergence can still be observed.

However, the lack of a widely endorsed treaty and of competing alternative models cannot alone explain th EU's influence on third countries' laws and ability to regulate global markets. The willingness of the EU to be a model and to foster its external influence is the second pillar of the analysis.

27. *Id.*

28. *See Id.* at 845.

29. Greenleaf, *supra* note 12.

30. *Id.* at 70.

31. *See generally* Eric Lachaud, *The General Data Protection Regulation and the rise of certification as a regulatory instrument*, 34 COMPUTER L. & SECURITY REV. 244 (2018).

32. Merav Griguer, *Data protection in Africa: where do we stand one year before GDPR?*, BIRD & BIRD (Jul. 2017), https://www.twobirds.com/en/news/articles/2017/global/africa-newsletter-june/protection-des-donnees-personnelles-en-afrique-meig [https://perma.cc/6XZC-SUEL]; *see also* YouTube: CPDP 2018: Convention 108: Convergence and Expansion (Panel at the Computers, Privacy & Data Protection conference, Brussels, January 2018) (https://www.youtube.com/watch?v=yKKv4wtixQ0 [https://perma.cc/P9NT-2A6G]).

33. *See* Greenleaf, *supra* note 22.

34. *Id.* at 2.

B. An Influence Sought After by the EU

The EU started to build its Data Privacy model in 1995 with the Data Privacy Directive 95/46/EC (the Directive).[35] The Directive is characterized by a comprehensive data protection law with high standards, providing strong protection to personal information.[36] Although it tremendously increased convergence of rules among EU Member States, it did so in an imperfect way.[37] Despite some alignment, the specifics of these laws differed among jurisdictions. The result was a fragmented data protection landscape with legal uncertainty, unequal protection for data subjects, and unnecessary costs and administrative burdens for data controllers.[38] To eventually reach absolute convergence within the EU, it was necessary to adopt a regulation which would be directly applicable in the Member State's legal system.[39] This was accomplished in 2016 with the GDPR.[40] The GDPR not only fully harmonizes personal data protection in the EU (with the exception of certain areas left to Member States' discretion, such as the age of consent),[41] but it also overhauls the level of protection for personal data, increases sanctions, introduces the accountability principle, and explicitly states its extraterritorial application.[42]

35. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

36. *Id.* at 32.

37. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Affairs Committee and the Committee of the Regions, Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century,* at 3, COM (2012) 9 final (Jan. 25, 2012) ("Despite the current Directive's objective to ensure an equivalent level of data protection within the EU, there is still considerable divergence in the rules across Member States. As a consequence, data controllers may have to deal with 27 different national laws and requirements.")

38. *Id.*

39. EU officials stated that a driver for replacing the Directive by a Regulation was to reinforce the comprehensive law model by having a single rule applicable to every state in Europe, instead of a patchwork of laws implementing the Directive in their own terms. *See* Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIVACY L. 119–129, 128 (2012).

40. *See* 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"].

41. GDPR, Art. 8.1. *Id.* at 37 ("[…] the processing of the personal data of a child shall be lawful where the child is at least 16 years old. […] Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.").

42. For the sake of brevity, a detailed analysis of the content of data protection laws is beyond the scope of this article. *See generally id.*

As previously mentioned, cost-savings motivate several third countries to use the EU data protection legal framework as a model for their own laws.[43] Likewise, a country with an established legal rule may itself actively seek to be used as a legal model because it will receive several benefits from it. In business law for instance, sharing similar legal systems will make it easier for companies from the donor country to do business with firms from the transplant country.[44] Another benefit is that in serving as a model, a donor country can export it's values, such as those reflected in human rights law, to a third country.[45] In the field of personal data protection, apart from the prestige of being an influential regulatory superpower and the various benefits that may result from that status, the EU wants to globally protect what it considers to be fundamental rights.[46]

The protection of privacy and personal information are fundamental rights in the EU. Article 8 of the European Convention on Human Rights provides that "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[47] The First Article of Directive 95/46/EC mentions: "[…] Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[48] In Article 8, the Charter of Fundamental Rights in the European Union provides that everyone has the right to the protection of personal data, which should be processed on a legitimate legal basis such as consent, that everyone has the right of access to their personal data and the right to have it rectified, and that an independent authority shall control compliance with these rules.[49] The right to personal

43. Miller, *supra* note 26.

44. *See* Bradford, *supra* note 21, at 23-25.

45. MATHIAS SIEMS, COMPARATIVE LAW 235 (2 ed. 2018), https://www.cambridge.org/core/books/comparative-law/89953745336B9C5F061BC21F48EE0F04 [https://perma.cc/QUX3-VVWE]; s*ee also* Miller on the role of the donor: Miller, *supra* note 26, at 4-5.

46. Bradford, *supra* note 21.

47. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, *opened for signature* Nov. 4, 1950, E.T.S. 5, 11. Although the EU itself has not yet accessed to the ECHR, all Member States have ratified it and the EU recognizes the rights guaranteed by the ECHR as general principles of EU law. *See* Consolidated Version of the Treaty on European Union art. 6, Feb. 7, 1992, 2012 O.J. (C 326) 19.

48. *Supra* note 35, art. 1 (repealed 2018).

49. Charter of Fundamental Rights of the European Union art. 8, Dec. 7, 2000, 2012 O.J. (C 326) 397.

data protection is also asserted in Article 16 of the Treaty on the Functioning of the European Union ("TFEU").[50]

When the Treaty of Lisbon entered into force in 2009, the Charter of Fundamental Rights in the European Union was elevated to primary law.[51] Since then, "EU law [has been] given the tools to assert its values and interests at a global level regarding the Internet, as can be seen in the post-Lisbon judgments of the Court of Justice which rely on the [Treaty on European Union (TEU)], the TFEU, and the Charter to assert the global reach of EU law."[52] The promotion of these values is one of the core missions of the European Union. The TEU states that "in its relations with the wider world, the Union shall uphold and promote its values and interests […]."[53] The EU views these values as normatively desirable and universally applicable.[54] Among these values are: "respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, including the rights of persons belonging to minorities."[55] These values have been extended to the Internet in the last twenty years.[56] The TEU explicitly mandates the EU to advance its guiding principles (of which fundamental rights are a part of) throughout the world through EU's external action,[57] thereby implying a strong tilt towards establishing its regulatory clout.

The European Commission embraces this view and argues that the EU should "promote its data protection values and facilitate data flows by encouraging convergence of legal systems,"[58] with the goal "to foster convergence by developing high and interoperable personal data protection standards globally" [to contribute] to the

50. Consolidated Version of The Treaty on the Functioning of the European Union, art. 16.1, *opened for signature* Mar. 25, 1957, 2012 O.J. (C 326) 55.

51. Ottavio Marzocchi, The protection of fundamental rights in the EU, FACT SHEETS ON THE EUROPEAN UNION (2019), http://www.europarl.europa.eu/factsheets/en/sheet/146/the-charter-of-fundamental-rights [https://perma.cc/C3DG-7AQA] (last visited Oct. 10, 2019).

52. Christopher Kuner, *The Internet and the Global Reach of EU Law,* Law Society Economy Working Papers, at 12, Apr. 2017, https://papers.ssrn.com/abstract=2890930 [https://perma.cc/SC5R-9SFR]. *See generally* HIELKE HIJMANS, THE EUROPEAN UNION AS GUARDIAN OF INTERNET PRIVACY : THE STORY OF ART 16 TFEU, (2016).

53. *See* Consolidated Version of the Treaty on European Union art. 6, Feb. 7, 1992, 2012 O.J. (C 326) 17, 28.

54. Bradford, *supra* note 21, at 37.

55. Treaty on European Union, *supra* note 53, at 17.

56. Kuner, *supra* note 52 at 11.

57. Treaty on European Union, *supra* note 53, at 28.

58. *Communication From The Commission To The European Parliament And The Council, Exchanging and Protecting Personal Data in a Globalised World*, at 2, COM (2017) 7 final (Jan. 10, 2017).

more effective protection of individuals' rights.[59] EU officials have also expressed their desire for the GDPR to serve as an international standard. Věra Jourová, the European Commissioner for Justice, stated, "we want to set the global standard,"[60] and Giovanni Buttarelli, the European Data Protection Supervisor, expressed his hope that "during the period of a generation for which the GDPR is likely to apply, we will have achieved a common standard, a sort of digital gold standard."[61]

These elements show that the transplantation of EU rules on data protection is fostered by at least two motivating factors. The first factor is the need for third countries to enact new laws in this field. These countries are driven towards the most efficient legal rules and prefer to import these laws rather than venture to find a new approach (the cost-saving transplant identified by Miller).[62] The second factor is the incentive for the EU itself to encourage convergence of third countries with EU laws. This drives the Union to promote its values and protect fundamental rights in the wider world.

Compared to the EU model, the U.S. provides less protection to personal information through various laws that are limited in scope. In this situation, the U.S. can respond either by voluntarily converging with the EU, attempting to convince the EU to change its rules by using diplomacy, or suing the EU under the WTO, seeking a cooperative solution by example through promoting international standards, or doing nothing.[63]

The following discussion demonstrates that in the field of personal data protection, the U.S. chose to do nothing and declineddecline to change its minimalist approach because of conceptual differences on the right to privacy and data protection. The section also shows that despite U.S. inaction, there are signs of convergence that are nonetheless appearing and increasing, and

59. *Id*. at 11.

60. Mark Scott & Laurens Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, POLITICO (Jan. 31, 2018), https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/ [https://perma.cc/X2ZU-6J7A].

61. Giovanni Buttarelli, *The EU GDPR as a Clarion Call for a New Global Digital Gold Standard*, 6 INTERNATIONAL DATA PRIVACY LAW 77–78 (2016).

62. While cost-saving is arguably the most evident of the motivation for transplanting EU rules, other reasons can come into third-countries decisions, such as the legitimacy gained when enacting laws based on those widely recognized as the most protective, or to reduce the transaction costs existing because of the difference between legal systems. Miller, *supra* note 26, at 843-854.

63. Bradford, *supra* note 21, at 50.

that the U.S. may attempt to counter the EU's global regulatory clout by formally establishing an alternative model.

II. THE DIRECTION OF US LAWS ON DATA PRIVACY

A. The Minimalist US Approach

As mentioned above, the EU and the U.S. have different philosophies on personal data protection, leading to divergence.[64] Privacy and personal data protection are fundamental rights in the EU, whereas in the U.S., those rights are grounded in consumer protection regulations.[65] While the United States Constitution provides some privacy protection, that protection is limited. In the U.S. Constitution, the Fourth Amendment[66] only protects U.S. citizens and long-term U.S. residents against unreasonable searches and seizures by the government and does not grant an actual broad right to privacy.[67] Conversely, the First Amendment can actually sometimes be used to restrict information privacy by protecting the freedom of expression.[68]

The U.S. Constitution and its supporting body of jurisprudence does not provide adequate privacy protection, especially in light of continuing technological development. The absence of a constitutional right to privacy will result in various privacy-protecting acts clashing with well-established constitutional rights. As a result, these Acts and their protection of privacy will be watered-down if not stricken outright.[69]

64. Gabriela Zanfir, *EU and US Data Protection Reforms. A Comparative View*, 7 EUROPEAN INTEGRATION REALITIES AND PERSPECTIVES 217, 218 (2012).

65. Shawn Marie Boyne, *Data Protection in the United States*, 66 THE AMERICAN JOURNAL OF COMPARATIVE LAW 299–343, 301 (2018) (explaining that the main leading enforcement agency in the U.S. for privacy is the Federal Trade Commission (FTC), whose authority is in principle limited to act against deceptive or unfair trade practices, pursuant to section 5 of the Federal Trade Commission Act. Even though the U.S. Congress has granted the FTC authority to enforce several sectorial laws, there is no equivalent to the EU requirement of an independent supervisory authority); Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are Stricter than Each Other for the Privacy of Government Requests for Information,*66 EMORY L.J. 617, at 628-29.

66. U.S. CONST., amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

67. Zanfir, *supra* note 64, at 218.

68. Paul M. Schwartz, *The EU-U.S. Privacy Collision: a Turn To Institutions and Procedures*, 126 HARVARD L. REV. 1966, 1976 (2013).

69. Avner Levin & Mary Jo Nicholson, *Privacy law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357, 367 (2005)..

Even if personal information is sometimes well-protected,[70] U.S. laws balance individuals' interests with those of state security agencies and of commerce.[71] In addition, the protection of personal information is primarily motivated by the protection of liberty.[72] Pursuant to that vision, "privacy is important inasmuch as it protects the liberty that is its foundation, and there is no reason and no need to protect privacy if liberty is not in danger."[73]

The right to privacy was first discussed in the U.S. in the 19th century by Samuel Warren and Louis Brandeis, in their article advocating for the right to be let alone in response to the development of a too enterprising press.[74] The country then had an important role in early global discussions on data protection.[75] But since then, it has been slow to develop its framework for the protection of personal information, resulting in a large number of sectoral rules focused on regulating specific areas such as healthcare, communications, and finance and credit.[76] Consequently, "privacy is protected in the US by means of a patchwork quilt made up of common law, federal legislation, the US Constitution, state law, and certain state constitutions,"[77] combined with industry self-regulation.[78]

There are sector-specific laws aimed at the private sector and those granting protection from the government. In the latter group, the Privacy Act of 1974 applies to data processing by the Federal government (but not state governments), the Electronic Communications Privacy Act of 1986 provides limited protection to individuals from the interception of their electronic communications, such as emails and other records, by government officials, and the Family Educational Rights and Privacy Act (FERPA) safeguards students at institutions receiving federal

70. Swire & Kennedy-Mayo, *supra* note 65, at 636.

71. STEPHEN COBB, DATA PRIVACY AND DATA PROTECTION: US LAW AND LEGISLATION (2016).

72. Levin and Nicholson, *supra* note 69, at 360.

73. *Id.* at 384.

74. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV. L. REV. 193-220 (1890) (using privacy rights already as a protection from technological evolutions, especially the development of the press and the associated portable cameras).

75. Schwartz, *supra* note 68, at 1969.

76. *Id.* at 1974–75.

77. Levin & Nicholson, *supra* note 69, at 360.

78. *Opinion 1/99 Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the United States Government: WP15*, at 2, ART. 29 WORKING PARTY (Jan. 26, 1999), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf [https://perma.cc/T2QV-DL7C] [hereinafter *Opinion 1/99*].

funding from the disclosure of their personal information without their consent, in addition to affording students the right to access and modify such information.[79] Among the main sectoral laws protecting against private actors, the 1996 Health Insurance Portability and Accountability Act (HIPAA) protects personal information related to an individual's health, and the Children's Online Privacy Protection Act of 1998 (COPPA) protects the privacy of children under the age of 13 against collection and misuse of personal data by commercial websites.[80] A wide range of other sectoral laws protect individuals' financial information, communications, video rental records, telephone and family information.[81]

This piecemeal approach, unpredictable and difficult to understand,[82] is considered unreliable by the Article 29 Data Protection Working Party ("WP29"), the group of EU Member States' that had supervisory authority on personal data protection until replaced by the European Data Protection Board upon enactment of the GDPR.[83] The WP29 acknowledged the divergence between the EU and the U.S. model by stating that the "patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union."[84]

In addition to different philosophies and legal instruments, the U.S. and the EU disagree on the substance and level of data protection. One of the main issues is that the U.S. does not define personal information in a uniform manner, whereas the EU broadly defines personal data as any information relating to an identified or identifiable natural person.[85] In the U.S., some instruments

79. Levin & Nicholson, *supra* note 69, at 362–63.
80. *Id.* at 366-67.
81. *Id.* at 363–67.
82. *Id.* at 361.
83. Under the GDPR, the WP29 is replaced by the European Data Protection Board ("EDPB"). *See generally Europe's New Data Protection Rules and the EDPB: Giving Individuals Greater Control*, EUR. DATA PROTECTION BOARD (May 25, 2018), https://edpb.europa.eu/news/news/2018/europes-new-data-protection-rules-and-edpb-giving-individuals-greater-control_en [https://perma.cc/F8RR-RE3B].
84. *Opinion 1/99*, *supra* note 78, at 2.
85. Regulation (EU) 2016/679, *supra* note 40, at 33.

include "identifiability" as a factor,[86] but "identifiable" personal information may fall outside the scope of certain privacy laws.[87]

In fact, neither federal nor state law agree on a single term that identifies the basic category of personal information, which makes the concept of personal data uncertain.[88] Beyond the scope of applicable laws, the U.S. differs from the EU on the existence and content of various core data protection principles. Some of them are present in both legal systems (though stronger in the EU), while others are found exclusively in the EU model.[89] In the first category, data minimization, transparency, and data quality are stricter in the EU but do exist in the U.S. In the second category, principles such as additional protection for sensitive data, restrictions on onward transfers, the need for a legal basis for data collection and processing, oversight by an independent supervisory authority, and limits on profiling and automated decision-making are typically not found in U.S. laws.[90]

Therefore, signs of convergence between the U.S. approach and the EU model at the federal level are barely existent. On that note, it is worth mentioning one missed opportunity to increase the rapprochement of laws: The Consumer Privacy Bill of Rights ("CPBR"). The Obama administration first presented a blueprint for the bill in 2012[91] and then a draft bill in 2015.[92] Though it provided the opportunity for convergence with the EU model, it never became law.[93]

In proposing the CPBR, the Obama administration sought to create comprehensive and globally recognized data privacy

86. *See, e.g.*, *Guidance on the Protection of Personal Identifiable Information*, U.S. DEP'T OF LABOR, https://www.dol.gov/general/ppii [https://perma.cc/REW7-96S4] (last visited May 30, 2019).

87. Paul Schwartz & Daniel Solove, *Reconciling Personal Information in the United States and European Union*, 102 CAL. L. REV. 877, 888 (2014). The key difference here being that "identifiability" refers to the *propensity* of the data to be identifiable.

88. *Id.*

89. Schwartz, *supra* note 68, at 1976.

90. *Id.* at 1976-78.

91. THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 23, 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/Y28E-WJQK] (CPBR blueprint).

92. OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION DISCUSSION DRAFT: CONSUMER PRIVACY BILL OF RIGHTS ACT OF 2015 1 (2015), https://obamawhitehouse.archives.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf [https://perma.cc/2EWB-U3B2] (CPBR draft).

93. Zanfir, *supra* note 64, at 218; *see also* Céline Castets-Renard, *Privacy Shield: Toward a Strong Personal Data Protection Between the US and the EU?*, 14 LA REVUE DES JURISTES DE SCIENCES PO - HIVER 109, 110 (2018) (acknowledging U.S. role in early global privacy debates but recognizing continued divergence with EU).

principles[94] aimed at palliating the lack of "a clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models."[95] The references to the "commercial world" and "consumer data privacy" mark a different rationale from the EU approach focused on broader fundamental and human rights protection.[96] However, the CPBR did contain a definition of "personal data" similar to the one used in the EU[97] and would have brought elements of convergence with EU laws with regard to several aspects, such as providing more control to the individual on data collection and processing, and improved requirements addressing consent, transparency, and accountability.[98]

Today, the U.S. approach is lacking because it does not seek to protect privacy as a fundamental right as the EU does. The main consequence is that the protection of personal data is always balanced against other interests such as commerce or free speech.[99] This explains the U.S. decision not to have a comprehensive data protection law in favor of several narrower laws as well as its decision to provide lower protection to personal information so as to avoid hindering other interests.

However, this approach has difficulty addressing today's omnipresence of personal data processing, the risks associated with lack of data security, and the misuse of that data. Following several data breaches and privacy scandals, such as those involving Equifax (a data breach that impacted more than 145 million U.S consumers in 2017),[100] Facebook (in the Cambridge Analytica scandal revealed in 2018, personal data was collected from millions of users without their consent, for political purposes),[101] and Uber (in 2016, the firm hid a data breach affecting 57 million users and

94. *Id.* at 9.
95. THE WHITE HOUSE, *supra* note 91, Foreword.
96. *See supra* section I.B.
97. Zanfir, *supra* note 64, at 220.
98. *Id.* at 221.
99. Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L. 365, 383 (2012).
100. Brian Fung, *Equifax's Massive 2017 Data Breach Keeps Getting Worse*, WASH. POST (Mar. 1, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/ [https://perma.cc/Q5Q3-YZZ8].
101. Alix Langone, *Facebook's Cambridge Analytica Controversy Could Be Big Trouble for the Social Network. Here's What to Know*, TIME (Mar. 20, 2018), https://time.com/5205314/facebook-cambridge-analytica-breach/ [https://perma.cc/QD3T-LUZ5].

paid hackers $100,000 to delete the data),[102] the U.S. approach on the matter has been increasingly scrutinized for being insufficient and even hurting the online economy.[103]

As a consequence of the absence of legal protections to prevent those scandals, initiatives from privacy advocates to strengthen the legal data protection framework have gained popularity and support.[104] The most notable of these evolutions reflecting convergence with EU rules can be observed in California regulation as well as that of several other states.

B. Convergence Coming from US States

Despite federal resistance to issuing stricter privacy rules, several U.S. states enacted laws showing signs of convergence with the EU model. It is suggested that those laws are responses to the Trump administration's failure to enact stricter privacy protections, wherein blue states act independently passing legislation to better protect consumer rights.[105]

At the forefront of these developments in the U.S. is California. As far back as 1972, the Golden State included in its constitution the right of privacy among the inalienable rights of all people.[106] Many advancements in privacy protection found in the laws of other

102. Andy Greenberg, *Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach*, WIRED (Nov. 21, 2017), https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/ [https://perma.cc/2Y7A-KE24].

103. A recent study by the National Telecommunications and Information Administration shows that nearly half of U.S. Internet users refrain from online activities, like buying and selling goods or conducting financial transactions, due to privacy and security concerns. *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMM. AND INFO. ADMIN.: BLOGS (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities [https://perma.cc/Q9SY-USUY].

104. *See, e.g.*, Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/RF4V-U8XH] (describing the California Consumer Privacy Act which is modeled on a ballot initiative pushed by a real estate developer, Alastair Mactaggart, who secured more than 600,000 signatures from backers); Makena Kelly, *Advocacy Groups are Pushing the FTC to Break up Facebook*, THE VERGE (Jan. 24, 2019), https://www.theverge.com/2019/1/24/18195959/facebook-advocacy-groups-ftc-break-up-cambridge-analytica-scandal-data-breach [https://perma.cc/AEC5-YWFB] (reporting on the call from several advocacy groups to break up Facebook following privacy violations and data breaches).

105. *The Privacy Advisor Podcast: On Why CCPA is Bad Law and Suing Kanye West*, INT'L ASS'N OF PRIVACY PROF. (Aug. 10, 2018), https://iapp.org/news/a/the-privacy-advisor-podcast-on-why-cacpa-is-bad-law-and-suing-kanye-west/ [https://perma.cc/D3RY-Q5JP].

106. J. Clark Kelso, *California's Constitutional Right to Privacy*, 19 PEPP. L. REV. 327, 328-29 (1991).

states come from California, such as data-breach notification requirements.[107]

On June 28, 2018,[108] against the backdrop of the GDPR's first days of being in effect and scandals such as the case of Facebook-Cambridge Analytica,[109] California passed the California Consumer Privacy Act of 2018 ("CCPA"), with the goal to improve personal data protection for consumers.[110] The CCPA explicitly aims to protect the right of Californians by requiring for-profit entities to inform them as to what personal information is being collected about them, whether their data are sold or disclosed and to whom, to refuse the sale of their personal information, to have access to it, and to protect their right to equal service and prices, even if they elect to exercise their privacy rights.[111] Although it is the most rigorous privacy law in the country[112] and features important signs of convergence with the EU model, it features significant differences .

Being a consumer law, its scope is notably narrower than EU laws. A consumer under the CCPA means "a natural person who is a California resident,"[113] whereas GDPR does not have a residency requirement.[114] Entities covered by the CCPA are limited to for-profit organizations operating in California, above several

107. The California data security breach notification law (California S.B. 1386) was passed in 2002, before similar requirements appeared in the EU. *See* Jane K. Winn, *Are "Better" Security Breach Notification Laws Possible?*, 24 BERKELEY TECH. L.J. 1133, 1142-47 (2009).

108. For practical and political reasons, the Act has been adopted very fast by the California legislature. *See* Determann Lothar, *Analysis: The California Consumer Privacy Act of 2018*, IAPP (2018), https://iapp.org/news/a/analysis-the-california-consumer-privacy-act-of-2018/ [https://perma.cc/QP8W-7RJT] (last visited May 30, 2019); ERIC GOLDMAN, *An Introduction to the California Consumer Privacy Act (CCPA)* (2018), https://papers.ssrn.com/abstract=3211013 [https://perma.cc/68N5-SEZB] (last visited Jul 29, 2019).

109. Matthew Rosenberg, Nicolas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions,* N. Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html [https://perma.cc/ZM6M-QPYM];
Alastair Mactaggart, *A letter from Alastair Mactaggart, Board Chair, Californians for Consumer Privacy*, CALIFORNIANS FOR CONSUMER PRIVACY, https://www.caprivacy.org/about-us [https://perma.cc/P8AN-4B9D] (last visited Jul 6, 2019).

110. The California Consumer Privacy Act of 2018, CAL. CIV. CODE §1798.100-199, [hereinafter CCPA] (2020).

111. *Id.* at SEC.2 (i)(1)-(5).

112. Lindsey Tonsager & Weiss Nusraty, *California Adopts Expansive Consumer Privacy Law*, INSIDE PRIVACY (2018), https://www.insideprivacy.com/data-privacy/california-adopts-expansive-consumer-privacy-law/ [https://perma.cc/8V7H-FUQX] (last visited May 30, 2019).

113. CCPA *supra* note 110, at para.1798.140(g).

114. 2016 O.J. (L 119) Art. 4(1).

thresholds on revenues and amount of personal data processed.[115] In addition, certain elements of an EU-like comprehensive data protection law are outside the scope of the CCPA, such as protection for health information and publicly-available data.[116] The CCPA probably has an extraterritorial scope like the GDPR, but this will depend on how the requirement of doing business in California is interpreted, given that the definition is not as explicit as that within the GDPR.

The CCPA applies to an entity that "does business in the State of California."[117] Comparison with other California rules defining this "doing business" requirement shows that extraterritorial applicability of the CCPA is likely.[118] Apart from the scope, the main topics of divergence are the absence of a requirement for a legal basis for data collection and processing, a right of action for individual that is limited to security issues in the context of a data breach, differences on the concept of supervisory authority, and the nature of penalties.

Apart from those remaining differences, it is worth focusing on the convergence between the CCPA and the EU model. First, personal information is similarly defined in California as in the EU as information "that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[119] This definition goes beyond previous U.S. and California laws. Other data protection elements where the CCPA is converging with the GDPR are pseudonymization, special protection for children, and especially rights for individuals.

The right to erasure extends to data processors, and the right to information requires that individuals should be informed of the categories of data collected, for what purpose, and the content of their rights. Both laws provide a right of access that extends to data portability and require data controllers to have mechanisms in place to ensure that access to personal data is granted to the right

115. CCPA *supra* note 110, at para. 1798.140(c)(1)(A-C).

116. *Id.* at para. 1798.140(o)(2) and 145(c).

117. *Id.* at para. 1798.140(c)(1); s*ee also id.* at para. 1798.145(a)(6) (states that CCPA won't apply if the "commercial conduct takes place wholly outside of California," *i.e.* "if the business collected that information while the consumer was outside of California, no part of the sale of the consumer's personal information occurred in California, and no personal information collected while the consumer was in California is sold.").

118. ALICE MARINI ET AL., *CCPA, Face to Face with the GDPR: An in Depth Comparative Analysis* 8–9 (2018), https://fpf.org/2018/11/28/fpf-and-dataguidance-comparison-guide-gdpr-vs-ccpa/ [https://perma.cc/VC2N-2KVM] (last visited Feb. 10, 2019).

119. CCPA *supra* note 110, at para.1798.140(o)(1)

person. In addition, like the GDPR, the CCPA requires that personal data is only disclosed to service providers if done pursuant to a written contract, specifying how the data is to be processed.

While CCPA requirements are not identical to those in the GDPR, they are closer to it than they were under previous laws. The fact that they tend to become more similar is what convergence is all about, as to converge means "to tend to meet at a point."[120]

Many other states are also improving their personal data protection legal framework, though at a slower pace than California and still through laws that are limited in scope. Delaware, Missouri, Arizona, Connecticut, Nevada, Massachusetts, and Colorado are examples of U.S. states that have passed laws to address the various issues related to data protection such as the privacy of children, e-book readers, website visitors and personal data held by Internet service providers, false and misleading statements in website privacy policies, and the monitoring of employee e-mail and Internet access.[121] Provisions on data breach notifications are also being strengthened in several states.[122] In

120. *Converge*, OXFORD ENGLISH DICTIONARY, https://en.oxforddictionaries.com/definition/converge [https://perma.cc/RXK3-3M8X] (last visited Mar. 16, 2019).

121. *See State Laws Related to Internet Privacy*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx [https://perma.cc/JSV2-QBN7] (last visited May 30, 2019) (The National Conference of State Legislatures (NCSL) keeps track of some of the most important state laws related to data protection, divided by categories).

122.The NCSL notes that "all 50 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information. Security breach laws typically have provisions regarding who must comply with the law (*e.g.*, businesses, data/ information brokers, government entities, etc); definitions of 'personal information' (*e.g.*, name combined with SSN, drivers license or state ID, account numbers, etc.); what constitutes a breach (*e.g.*, unauthorized acquisition of data); requirements for notice (*e.g.*, timing or method of notice, who must be notified); and exemptions (*e.g.*, for encrypted information)." Among the most recent, the Maryland Personal Information Protection Act (MPIPA) which will go into effect on October 1, 2019, requires notification of affected persons within 45 days; New Jersey amended its data breach law (S-52, coming into effect on September 1, 2019) to expand the definition of "personal information" that would require a company to issue a notification in case of a breach; Washington also expanded its data breach notification law (RCW 19.255.010), to reduce the timeframe for notification from 45 to 30 days, effective on March 1, 2020. *See generally Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURE, http://www.ncsl.org/research/telecommunications-and-information-

South Carolina for example, the Insurance Data Security Act mandates that the licensee shall notify the Director of the Department of Insurance within 72 hours of a cybersecurity event, the same timeframe as in the GDPR.[123] Following California's lead, bills strengthening privacy rights are being proposed across the U.S.[124]

The case of Colorado exemplifies the recent direction of states on data privacy, where protection for personal data was initially minimal but privacy scandals spurred the need for new rules. Until 2018, safeguards against the misuse of personal information in the Colorado Consumer Protection Act[125] mostly consisted of no-call lists of Colorado residential subscribers objecting to receiving telephone solicitations for marketing purposes[126] and a requirement for companies to disclose a potential security breach to affected Colorado residents within a reasonable timeframe.[127] Then, as in California, privacy-related scandals like the Equifax data breach and the Facebook-Cambridge Analytica case put the relevance of those laws into question, as sponsors for a new bill[128] cited those cases as motives for strengthening Colorado's rules.[129]

Although personal information in the new law receives a narrow definition compared to the CCPA and the GDPR,[130] the new law increases privacy in several ways. The most significant improvements are stricter data breach notification rules;[131] a

technology/security-breach-notification-laws.aspx [https://perma.cc/E94Z-5NLA] (last visited Jun 30, 2019).

123. S.C. CODE ANN. §38-99-40(A) (2019).

124. *See* Jeewon Kim Serrato & Susan Ross, *Nevada, New York and other states follow California's CCPA*, DATA PROTECTION REPORT (June 6, 2019), https://www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/ [https://perma.cc/4KJS-ACAP].

125. COLO. REV. STAT. §6-1-101-1121 (2019).

126. COLO. REV. STAT. §6-1-904-905 (2019).

127. Lauren Lambert Schreier, *Data Privacy in Colorado*, COLORADO LEGISLATIVE COUNCIL STAFF (Nov. 2014), http://leg.colorado.gov/publications/data-privacy-colorado-2014 [https://perma.cc/WHU4-T4KU].

128. H.R. 18-1128, 71st Gen. Assemb., (Colo. 2018).

129. *House OKs Bridges Bill Cracking Down on Data Breaches*, COLORADO HOUSE DEMOCRATS (Apr. 20, 2018), https://www.cohousedems.com/house-oks-bridges-bill-cracking-down-on-data-breaches/ [https://perma.cc/F7RC-9DTJ] (quoting Rep. Jeff Bridges, prime sponsor of the bill: "The massive data breach at Equifax and the disregard shown by Facebook for protecting consumer privacy underscores the need for this bill.").

130. H.R. 18-1128, 71st Gen. Assemb. §§ 1(2)(b),3(1)(g)(I)(A) ("Personal identifying information" is defined as a Colorado resident's first name or first initial and last name in combination with "personal identifying information" such as the numbers assigned to a person (social security number, ID card number, driver's license number…) and exclude publicly available information.).

131. *Id.* at § 3(2). (Notification to the affected Colorado residents must now be made within thirty days after the determination that a breach occurred and include a list of

requirement to take reasonable measures, appropriate to the nature of the personal data, to ensure the security of personal information;[132] and the responsibility for the company to ensure that its third-party service provider implements and maintains reasonable security procedures and practices.[133]

As a result—whereas in the EU one law governs the whole market—in the U.S., companies must navigate a large number of state laws. The fragmentation described in this article is cited as one of the key reasons for federal lawmakers seeking to implement a nationwide law.[134] As demonstrated, the federal government is now facing the implementation of new laws at the U.S. state level, the GDPR in Europe with its worldwide influence, and an expectation to respond to several recent scandals (Equifax, Facebook & Cambridge Analytica, Uber, etc.). To counter the somewhat limited protection provided for in the U.S., Democratic Senators have introduced a resolution calling for the application of GDPR requirements to U.S. citizens.[135] Support for a "U.S. GDPR" even comes from top executives with major U.S. companies, such as Apple and Cisco, which have publicly advocated for a comprehensive data protection law in the U.S.[136]

In the first months of 2019 alone, the 116th U.S. Congress has seen several reports and initiatives for strengthening personal data protection, typically closely aligned with the most recent EU developments. The U.S. Government Accountability Office (GAO), a bi-partisan government agency that provides auditing, evaluation, and investigative services for Congress, published a report, which states, "recent developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider comprehensive Internet privacy legislation,"[137] with the

mandatory information such as the date of the breach and the personal information acquired).

132. *Id.* at § 2(1).

133. *Id.* at § 2(2).

134. Olivia Gazis, *Trump Administration Takes New Steps on Crafting Data Privacy Framework*, CBS NEWS, (Sept. 25, 2018), https://www.cbsnews.com/news/trump-white-house-data-privacy-proposal-national-telecommunications-information-administration/ [https://perma.cc/96JK-6QVR].

135. S. Res. 523, 115th Cong. (2018) ("Encouraging companies to apply privacy protections included in the General Data Protection Regulation of the European Union to citizens of the United States.").

136. Don Reisinger, *Cisco, Like Apple, Calls for a GDPR-Like Federal Privacy Law for U.S.*, FORTUNE (Feb. 8, 2019), http://fortune.com/2019/02/08/cisco-federal-privacy-law/ [https://perma.cc/VL72-87HH].

137. U. S. GOVERNMENT ACCOUNTABILITY OFFICE, *Internet Privacy: Additional Federal Authority Could Enhance Consumer Protection and Provide Flexibility* (Jan. 15, 2019), https://www.gao.gov/products/GAO-19-52 [https://perma.cc/8ZPW-732U] (This report was requested by the House Energy and Commerce Committee in 2017).

FTC being in charge of enforcing the new rules. The Social Media Privacy Protection and Consumer Rights Act,[138] introduced in January 2019, would require covered entities to notify an individual of a data breach within 72 hours, faster than previous laws and aligned with the GDPR. Also introduced in January 2019, was the American Data Dissemination Act,[139] which would extend to internet service providers the requirements imposed on federal agencies under the Privacy Act of 1974.

A possible solution to the legal fragmentation in the U.S. would see Congress pre-empting state laws by enacting a federal law on data protection.[140] The question of whether a federal law should overrule state regulation is the subject of much debate, but most observers tend to prefer an approach that would help reduce the patchwork of U.S. laws.[141]

Officials have expressed that the Trump administration is now working towards what could be the first comprehensive data protection law in the U.S.[142] Such a law, as described by the White House, "aims to craft a consumer privacy protection policy that is the appropriate balance between privacy and prosperity […] We look forward to working with Congress on a legislative solution consistent with our overarching policy."[143] The quality and strength of the EU approach has driven privacy proponents to advise the Commerce Department to take it as a model for a potential new

138. Social Media Privacy Protection and Consumer Rights Act of 2019, S. 189, 116th Cong. (2019).

139. American Data Dissemination Act of 2019, S.142, 116th Cong. (2019).

140. Sara Merken, *FTC Needs More Clout to Police Data Privacy, Schakowsky Says*, BLOOMBERG (Jun. 5, 2019, 3:10 PM) https://news.bloomberglaw.com/privacy-and-data-security/ftc-needs-more-clout-to-police-data-privacy-schakowsky-says [https://perma.cc/9TJY-J6BR].

141. Stephanie Condon, *Congress Considers a National Standard for Data Privacy*, ZDNET (Feb. 26, 2019, 10:00 AM), https://www.zdnet.com/article/congress-considers-a-national-standard-for-data-privacy/ [https://perma.cc/Q7HZ-43DX]; *see also* the op-ed by Senator Marco Rubio, where he states that "a state-by-state patchwork of laws is simply not an effective means of dealing with an issue of this magnitude. Internet data is unquestionably interstate commerce, and it is the responsibility of Congress to take appropriate action." Marco Rubio, *Congress Needs to Address Consumer Data Privacy in a Responsible and Modern Manner*, THE HILL (Jan. 16, 2019, 8:20 AM), https://thehill.com/blogs/congress-blog/technology/425557-congress-needs-to-address-consumer-data-privacy-in-a [https://perma.cc/MQ45-EA4M].

142. Shannon Vavra, Kim Hart & David McCabe, *Scoop: The White House Looks to Coordinate Online Privacy Plan*, AXIOS (June 20, 2018), https://www.axios.com/scoop-the-white-house-looks-to-coordinate-online-privacy-plan-a51691cf-78d9-466e-8deb-27a66b1843c7.html [https://perma.cc/MEV3-VNB2].

143. David Shepardson, *Trump Administration Working on Consumer Data Privacy Policy*, REUTERS (July 27, 2018, 3:36 PM), https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK [https://perma.cc/QA63-882P].

regulation, while U.S. businesses push for lesser requirements than what is found in the EU.[144]

A nationwide data protection law would mark a shift in the U.S. approach and bring much-needed clarity to the U.S. legal framework on this issue, but it would not necessarily mean stronger protection for personal information. Future comparative studies on the data protection legal frameworks in the EU and the U.S. will indicate whether importation of EU rules, which can currently be observed at the state level, may also occur at the federal level in the U.S. This potential new law could be a basis for proposing an alternate model for data protection[145] and challenging the EU approach and influence.

CONCLUSION

This article first discussed the reasons behind the EU's global influence in the field of data protection. I included a discussion of earlier scholarly literature on legal transplantation and identified motivations, especially cost-saving, that apply in this context because many third countries import EU rules into their own laws. In addition, whereas past researches focus on legal transplantation from the angle of the recipient country, I focused instead on the point of view of the donor, the EU in this case. This analysis conceptualized that the EU itself needs to be influential to achieve its own policy objectives of fundamental rights protection, and actively encourages convergence with its laws to foster the protection of personal data. The EU is successful in doing so partly because of the lack of a competing model that third countries could look to.

The U.S., with a large market and an ability to regulate efficiently, could present this alternative model. However, to-date, the U.S. has chosen an approach that is difficult to follow and only provides minimal protections for personal data, which does not fit the need of most third countries looking to improve their protection and to enact new laws. The difference between the EU and the U.S.

144. Tony Romm, *The Trump Administration is Talking to Facebook and Google About Potential Rules for Online Privacy*, WASHINGTON POST (July 27, 2018), https://www.washingtonpost.com/technology/2018/07/27/trump-administration-is-working-new-proposal-protect-online-privacy/ [https://perma.cc/3UWT-ALUJ].

145. The idea of a potential shift in the US approach and the incertitude regarding its outcome – whether it will result in greater convergence with EU rules or not – is shared in the data protection experts' community. *See, e.g.*, Jules Polonetsky, LINKEDIN (July 2018), https://www.linkedin.com/feed/update/urn:li:activity:6428698510538866688/ [https://perma.cc/7SQM-U4FX] (Jules Polonetsky's statement on this issue on LinkedIn).

approach is mostly due to the conceptual differences as for the basis of the right of protection of personal data.[146] Personal information protection is not a fundamental right in the U.S., and therefore, is often overshadowed by other interests—explaining why U.S. laws on this issue are always narrow in scope and offer lesser protections.

Although most research only underlines the *differences* between both sides of the Atlantic, this article highlighted examples showing *convergence* of U.S. laws towards the EU model. At the federal level, it is limited, and even withdrawn before being applicable, as was the case for the CPBR. However, turning to U.S. state laws, this research identified that instances of tangible convergence are happening and increasing. The most recent developments in this trend could prompt the federal government to enact a nationwide law in the near future. A federal law could contain elements from the EU model, as do the state laws, but also effectively entrench important differences. A goal could be to challenge the EU's influence on the wider world and even attempt to prevent its rules from becoming, de facto, the global norm in this domain. The convergence between U.S. and EU laws on data protection is an issue that goes beyond the legal realm and should be closely monitored.

146. *See supra* section II.A.