Volume 123 | Issue 1 Article 5

September 2020

The Balkanization of Data Privacy Regulation

Fernanda G. Nicola
American University Washington College of Law

Oreste Pollicino
Bocconi University

THE BALKANIZATION OF DATA PRIVACY REGULATION

Fernanda G. Nicola and Oreste Pollicino***

---

* Professor of Law, American University Washington College of Law and Permanent Visiting Professor at iCouts, Center of Excellence funded by the Danish National Research Foundation. I would like to thank for their comments Daniela Caruso, Francesca Bignami, and Hugh Stevenson and for their stellar research and editing assistance Monica Carranza, Min Ji Kim, Timothy Schmeling, and Katerina Dee. Errors are mine only.

** Professor of Law and Director LL.M. in Law of Internet Technologies, Bocconi University in Milan, Italy. I would like to thank the Colleagues already mentioned for their very valuable comments and Giovanni De Gregorio for the editing assistance. Errors are mine only.

I. INTRODUCTION

As global data flows are inevitable, the increasing power of the European Union's innovative data privacy regulation, the General Data Protection Regulation ("GDPR")[1] that entered into force on May 25, 2018, is becoming evident to the world.[2] The GDPR has not only influenced other countries to adopt new privacy regulations,[3] but it has also triggered enormous compliance obligations, especially by United States ("U.S.") companies doing business in Europe. The GDPR has a significant territorial and extra-territorial scope that covers data processing not only within the European Union ("EU") and for its consumers[4] but also where data is processed outside of Member State territory with respect to EU citizens.[5] The GDPR regulates how companies, public organizations, governments, and businesses can use and process personal data, including anything from data collection, mining, data aggregation, or sharing of data.[6] For these reasons, the efforts of businesses and their lawyers to comply with the recently adopted GDPR to avoid its harsh penalties have strengthened the so called "Brussels Effect,"[7] namely the EU's ability, as characterized by Anu Bradford, to unilaterally influence global regulatory standards because of its

---

1 General Data Protection Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 34 (EU), art. 51(4) [hereinafter GDPR].

2 *Major GDPR Fine Tracker—An Ongoing, Always Up-to-Date List of Enforcement Actions*, COREVIEW, https://coreview.com/blog/alpin-gdpr-fines-list/ (last visited Aug. 10, 2020).

3 *See* Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 777 (2019) (citing Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 77 (2011)).

4 GDPR, *supra* note 1, art. 3(1)–(2).

5 *Id.* art. 3(2)(b).

6 *See What Does It Do?*, GDPR, https://gdprexplained.eu (last visited Sept. 6, 2020).

7 *See* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 8 (2012).

large market.[8] However, the breadth and the scope of the Brussels Effect and its regulatory influence remains unclear. Across the Atlantic, the need to regulate data privacy has exploded due to the increasing litigation against Facebook.[9] This led to the first relatively sizable Federal Trade Commission ("FTC") fine while sparking more congressional action towards a federal data privacy bill.

If the GDPR has led to awareness of and compliance with data protection regulation for U.S. consumers, state legislatures have taken new important measures to regulate consumer privacy. Bills like the California Consumer Privacy Act ("CCPA"), which entered into force on January 2020, provide a sectoral model, narrower than the GDPR,.[10] However, U.S. state legislatures are far from taking a comprehensive regulatory path similar to the GDPR. Many states are committed to raising the data privacy protections by following what David Vogel has called, with respect to environmental legislation, the "California effect,"[11] which is spreading rapidly across U.S. jurisdictions through the CCPA.

The non-convergence of data privacy regulation between the EU and the U.S. can be traced back to the different underlying cultural and legal attitudes,[12] the diverse political economy regimes towards data privacy, and the path dependencies of more or less decentralized regulatory systems.[13] In an effort to clarify the GDPR, this Article explains how the EU's decentralized administrative structure also has a centralized constitutional adjudication by the Court of Justice of the EU ("ECJ"). It has inevitably contributed some implementation features to the GDPR. This in turn makes it difficult, if not impossible, to export the European data privacy regulation even in a federal polity like the U.S.

The complexity of the GDPR architecture is difficult to replicate and includes an uneven implementation as well as open-ended rules for the Member States to transpose further into domestic legislation.[14] Besides, the harmonizing

---

8 *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? 176 (2006).

9 Litigation on data privacy has highlighted the concerns regarding the processing of data by social media. In April 2020, the United States Court of Appeals for the Ninth Circuit ruled that Facebook users have a reasonable expectation to privacy and can bring suit against the social media platform for tracking of web browsing which violates their privacy. *In re* Facebook, Inc. Internet Tracking Litig., 956 F.3d 589 (9th Cir. 2020). According to Chief Judge Thomas, "Facebook set an expectation that logged-out user data would not be collected, but then collected it anyway." *Id.* at 602.

10 CAL. CIV. CODE §§ 1798.100–80 (West 2020).

11 *See* DAVID VOGEL, TRADING UP 248 (1995).

12 James Q. Whitman, *Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1153, 1155–57 (2004); *see also* 47 U.S.C.A § 230 (West 2020).

13 *See* COMPARATIVE ADMINISTRATIVE LAW 1 (Susan Rose-Ackerman et al. eds., 2d ed. 2019); COMPARATIVE LAW AND REGULATION 7 (Francesca Bignami & David Zaring eds., 2018).

14 *See, e.g.*, GDPR, *supra* note 1, arts. 6, 9.

jurisprudence of the ECJ has strengthened fundamental rights and the dignitary approach to data privacy embedded in the GDPR. This has led to inevitable regulatory choices on the right to be forgotten often in opposition to the right of free speech that remains at the core of the U.S. legal regime.[15] If the dignitary dimension of data privacy as a fundamental right derives from the German constitutional tradition,[16] U.S. consumer privacy privileges of free choice and liberty are compatible with free speech protections.[17] Finally, embedded in some of its political economic regime, the GDPR ex-ante regulatory approach with the right to opt-in[18] departs from the ex-post regulatory CCPA approach with the right to opt-out. This latter approach offers a limited control to monitor the collection or processing of consumer data unless the business is aware that the consumer is under 16 years of age.[19]

This Article deploys some of the findings of the comparative administrative law literature and the theory of institutional change[20] to show that despite the fact that the GDPR is globally relevant for companies and lawyers concerned with data privacy compliance, its adoption among U.S. regulators is highly unlikely. This comes from the structural (and constitutional) difference of values underpinning data privacy across the Atlantic. It is not by chance that, in the consumer protection field, the CCPA emerged as a powerful alternative in the U.S., showing that once again the California Effect, described by Vogel in the realm of environmental law, is crucial to state and federal regulators alike. The CCPA adopts a less dignitary but consumer-oriented approach to data privacy regulation based on political, economic choices entailing ex-post market intervention, more active consumer litigation, and eagerness to balance consumer protections with economic incentives for online platforms in its jurisdictions. This inevitable Balkanization of data privacy regulation will create discrepancies in regulations and new costs to businesses in addition to greater experimentation in the realm of data privacy. This will train regulators and the courts to openly engage with the distributive costs of data privacy, whether limiting or enhancing access to platforms, their content, or individual rights. The current state of data privacy regulation in the U.S. shows more broadly that the reception and transfer of the GDPR to other countries, despite its adequacy and its regulatory innovation, remains uncertain because of administrative path dependencies and the uneven enforcement of the GDPR in the EU.

---

15 *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

16 *See* Francesca Bignami & Giorgio Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, 78 LAW & CONTEMP. PROBS. 231, 264 (2015).

17 *See id.*

18 GDPR, *supra* note 1, art. 15(3).

19 *Id.* arts. 4, 32.

20 *See* James Mahoney & Kathleen Thelen, *A Theory of Gradual Institutional Change*, *in* EXPLAINING INSTITUTIONAL CHANGE 1 (James Mahoney & Kathleen Thelen eds., 2010).

To achieve this purpose, Part II focuses on the EU and underlines how privacy and data protection have consolidated with a focus on the role of the ECJ in creating a fortress of personal data. Part III underlines how, despite the consolidation of privacy and data protection in the EU with the adoption of the GDPR, there are still areas of discretion in defining the boundaries of EU data protection law as shown by the role of the European Commission and the discretion of Member States in implementing some provisions. Part III also looks at how the ECJ has dealt with the jurisdictional issue in cases involving the extensions of EU law beyond territorial boundaries. Part IV focuses on the U.S. framework, precisely underlining the lack of an overarching federal data regulation, the centrality of the First Amendment, the role of consumer privacy, and the fragmentation of legislation at the national level. Part V provides a comparative perspective focusing on specific problems characterizing the approaches to data privacy across the Atlantic.

II. EU CONVERGENCE IN DATA PRIVACY

A. Historical Perspective of Data Privacy in the EU and the U.S.

To fully understand the issue of the scope of the GDPR and of the EU digital right to privacy being implemented beyond the borders of the EU, in a sort of extraterritorial effect, it is necessary to develop some premises. Precisely, it is worth focusing on the dynamic force of the European fundamental right to data protection and privacy in the digital world and the cleavage between the European vision of the right to privacy online and data protection and the American one.

Regarding the protection of fundamental rights of privacy and personal data, if it is true that the milestone for the reconstruction of the birth and evolution of the protection of privacy and personal data is the "American" theorization of Justice Warren and Justice Brandeis,[21] it is also ascertained that, compared to the U.S. legal system, in Europe, the protection of personal data and digital privacy acquired the status of a fundamental right.[22] Actually, this fundamental right assumes the nature of a super fundamental right,[23] which seems not to find any limits in the territorial dimension of the EU, following EU residents even in the

---

[21] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[22] In the ECHR system, see S. & Marper v. United Kingdom 2008–V Eur. Ct. H.R. 167. In the EU system, see Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen, 2010 E.C.R. I-11063.

[23] In "data privacy–oriented" case law of the European Court of Justice, the nature of a "super" fundamental right could be confirmed by the lack of any reference to freedom of information in the reasoning of the Court, that does not even mention Article 11 (freedom of expression) in its judgments. It cited the economic freedoms a few times, but even this balance soon disappeared. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014).

data processing outside the EU territory, and does not meet many limits in the balancing process between fundamental rights.

This evolution started in the second half of the twentieth century in the European Convention on Human Rights system. In this case, the right to privacy has been codified, and the system looks at it as a sort of habeas corpus concerning a person's spatial and relational projections.[24] As in the U.S., in the European constitutional framework, the recognition and codification of the right to privacy were originally made along the "negative" line, that is the recognition of the citizens' right to have their own private life respected.[25] However, in the following decades, this right underwent a deep transformation. Indeed, because of an acceleration of technology, a "positive" dimension of the right to the protection of personal data has enriched the "negative" dimension, typical of the right to privacy. This widening of the right to privacy to include protection of personal data has marked an expansion of a right initially limited to the "traditional" concept of privacy.[26] In this scenario, the European Court of Human Rights has played an important role in addressing technological changes and the challenges of online data processing.[27]

Against this background, the institutions of the then European Community were slower to codify a right to data protection or digital privacy, due to their original economical inspiration. For a long time in the EU legal system, individual rights have been recognized almost exclusively in order to ensure economic fundamental freedoms. As a consequence, in this context, it was difficult to make the protection of personal data a matter which could capture the attention of the European institutions for its direct impact on some fundamental rights.

---

[24] The first document at the European level that incorporated the right to privacy was Article 8 of the European Convention on Human Rights of 1950. *What Is the European Convention on Human Rights?*, EQUAL. & HUM. RTS. COMM'N (Apr. 19, 2017), https://www.equalityhumanrights.com/en/what-european-convention-human-rights.

[25] *See generally European Privacy Framework*, PRIVACY EUR., https://www.privacy-europe.com/european-privacy-framework.html (last visited Sept. 13, 2020); *The Right of Privacy*, EXPLORING CONST. RTS., http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html (last visited Sept. 13, 2020).

[26] The first step was the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data, the so-called Convention no. 108/1981. Finally, in 1987, the European Court of Human Rights clarified that the collection and processing of personal data must be included within the scope of Article 8. Leander v. Swed., 48 Eur. Ct. H.R. (ser. A) at 116 (1987); *see also* Amann v. Switz. 2000–II Eur. Ct. H.R. 245; S. & Marper v. U.K. 2008–V Eur. Ct. H.R. 167; M.M. v. U.K., 2012 Eur. Ct. H.R. 1906.

[27] In 2007, the web was formally included in the scope of application of Article 8. Copland v. U.K. 2007 Eur. Ct. H.R. 253; *see also* Węgrzynowski & Smolczewski v. Pol., 2013 Eur. Ct. H.R. 779; Bărbulescu v. Rom., App. No. 61496/08, ¶ 121 (Sept. 5, 2017), https://hudoc.echr.coe.int/spa#{%22fulltext%22:[%22\%22BARBULESCU%20v.%20ROMANIA\%22%22],%22itemid%22:[%22001-177082%22]}.

The breaking point was Privacy Directive 95/46.[28] Even if an economic dimension inspired it, the Directive was the first legal instrument in the EU legal system that promoted the harmonization of privacy and data protection rules at the EU level. It established both general principles concerning the processing of personal data and special rules based on specific and particular processing. In this scenario, the embryonic fundamental right to personal data protection and digital privacy started to acquire a concrete declination. Actually, the recognition and "constitutionalization" of this right was closely connected to the evolution of the EU's identity, and, perhaps, was an additional reason for the creation and consolidation of this super fundamental right. The right to the protection of personal data and digital privacy was finally codified in the Charter of Fundamental Rights of the EU and enshrined in Article 16 of the Treaty on the Functioning of the EU,[29] which provides the legal basis for the adoption of a new regulatory framework for the processing of personal data. Specifically, the Charter of Fundamental Rights of the EU devotes two provisions to the matter—Article 7, concerning the respect for private life and family life, and Article 8, regarding the protection of personal data.[30]

From the American perspective, it is clear that the right to privacy designed by Justices Warren and Brandeis as the "right to be let alone" has experienced a process of migration from the United States to Europe.[31] It has progressively acquired a dimension that does not exclusively protect the individual's expectation of privacy, but which sees it in the definition of a system of principles and rules for data protection—a further essential moment to protect the individual personality.

The European system created a *unicum*, an innovative and pervasive right to data protection and right to privacy, that has transfigured the Internet environment and has deeply influenced other legal systems generating a new

---

[28] 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, art. 25, 1995 O.J. (L 281) 31.

[29] OFF. J. OF THE EUR. CMTYS., CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION (Dec. 18, 2000), https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[30] CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION arts. 7, 8. Despite the attempt in the explanatory notes to the Charter to restrict the purpose of this provision to a mere reproduction of the existing *acquis* (see Explanations regarding Article 8 of the Charter), the contribution of Article 8 is quite significant. Not only has this provision permitted to provide the right to data protection with constitutional rank, it also did definitively emancipate the latter from its connection to the economic dimension that characterized, at least at the outset, Council Directive 95/46/EC. Joined Cases C-92/09 and C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert v. Land Hessen, 2010 E.C.R. I-11063. For more details, see Part II of this paper.

[31] Warren & Brandeis, *supra* note 21.

migration of this right.[32] However, this migration was preceded by a very pervasive case law of the European Court of Justice oriented at applying the European vision of the right to digital privacy on the Internet—or better on every hosting provider operating in Europe—and then was followed by European laws, above all the GDPR.

While the EU fundamental right to data protection and digital privacy wrapped its tentacles around the Internet, guaranteeing to EU citizens the protection of their European rights in the digital world, the U.S. system was stuck in the quicksand of the definition of the right to privacy, granting a right to data protection only in some specific fields.[33] Additionally, it has to be stressed that in the U.S., the main role in protecting users' data was played—at the federal level—by the FTC[34] and not by the Supreme Court of the United States.

In this scenario, we register a clash between the U.S. perspective and the European one. While the EU has established secondary rules (mainly the GDPR) to protect this new fundamental right to privacy and data protection and has accordingly regulated the Internet, the U.S. system has not introduced a general regulation. Moreover, it must be underlined how most Internet companies are based in the U.S. and are deeply influenced by the European rules since the European market is one of the most important for Internet companies.[35] It is above all concerning the U.S.-based giants of the web—Facebook and Google *in primis*—that extraterritorial scope takes shape[36] (but, for instance, some scholars have also analyzed how the super right to digital privacy could affect American newspapers and publishers[37]). This phenomenon concerns not only the U.S., but also the other two main actors in Internet regulation: the EU and China. China is

---

[32] Krystyna Kowalik-Bańczyk & Oreste Pollicino, *Migration of European Judicial Ideas Concerning Jurisdiction over Google on Withdrawal of Information*, 17 GERMAN L.J. 315, 318 (2015).

[33] Bignami & Resta, *supra* note 16. For a discussion on the "third party doctrine" and the general idea of privacy in the U.S., see Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C.L. REV. 1511, 1520 (2010).

[34] Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2267 (2015); *cf.* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 2–6 (2008).

[35] The European market has been an important market for tech giants to offer their services. Unlike other areas of the world which are subject to surveillance and control of digital activities like China, the liberal characteristics of the internal market have allowed tech giants to grow in Europe even if recently the Union has shown its intent to increase regulatory pressure over tech giants. Adam Satariano & Monika Pronczuk, *Europe, Overrun by Foreign Tech Giants, Wants To Grow Its Own*, N.Y. TIMES (Feb. 19, 2020), https://www.nytimes.com/2020/02/19/business/europe-digital-economy.html.

[36] Kimberly A. Houserb & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy*, 25 RICH. J.L. & TECH. 1, 6–7 (2018).

[37] Those scholars have also analyzed how this would be inconsistent with the First Amendment. Kurt Wimmer, *Free Expression and EU Privacy Regulation: Can the GDPR Reach U.S. Publishers?*, 68 SYRACUSE L. REV. 547, 561 (2018).

less connected with the other two systems in terms of cross-border data flow.[38] Therefore, the U.S. legal regime seems to be the most embroiled in the struggle for data protection online, and this topic can be understood in the broader one relating to the digital revolution.[39] In this perspective, the issue of the "Europeanization" [40] of data protection appears to be a very central topic that contains a challenge to the digital sovereignty of third countries, especially in the U.S.

With regard to data privacy, two aforementioned elements, the new fundamental right to digital privacy and data protection in the EU and the difference in regulations (and balance of fundamental rights) between the EU and the U.S., have generated a phenomenon called "Europeanization"—the application of EU law beyond the borders of the EU territory—of data protection online.

B. The Centralizing Role of the European Court of Justice

The GDPR is the rightful heir of a precise jurisprudence of the ECJ and the same court seems to be the main actor in the widening of the scope of EU law. In this perspective, digital privacy is probably the best-case study for analyzing the European "imperialism" on the Internet. In addition, the EU approach to digital privacy seems to be embraced by the ECJ in the free speech field, inaugurating new eventual trends in this perennial conflict between different digital sovereignties on the web.

To get a better understanding of the ECJ's approach when it comes to new technologies, the decision invalidating the data retention Directive 2006/24/EC must be analyzed.[41] *Digital Rights Ireland Ltd v. Minister for Communications*[42] appears to be a leading case concerning the grade of protection the Charter guarantees to the right to respect private life and to the protection of personal data. In this scenario, the European judges did not pass up the chance to invalidate, for the first time in the history of the European

---

[38] Nicholas F. Palmieri III, *Data Protection in an Increasingly Globalized World*, 94 IND. L.J. 297, 302–03 (2019); *see also* Griffin Drake, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CALIF. L. REV. 163, 175–76 (2017).

[39] *Cf.* Paul M. Schwartz, *The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 2003–08 (2013).

[40] The expression has been used both to describe the internal phenomenon of harmonization and centralization of data protection, Orla Lynskey, *The "Europeanisation" of Data Protection Law*, 19 CAMBRIDGE Y.B. EUR. LEGAL STUD. 252, 255 (2017), and to depict the tendency to widen the territorial scope of the EU Law. In this last sense the expression shall be used in this paper.

[41] Directive 2006/24, of the European Parliament and of the Council of 15 March 2006, 2006 O.J. (L 105) 54.

[42] Joined Cases C-293/12 and C-594/12, Digital Rts. Ir. Ltd. v. Minister for Commc'ns, ECLI:EU:C:2014:238, ¶¶ 1–5 (Apr. 8, 2014).

integration process, an act of secondary EU law as a result of its inconsistency with the European Charter of fundamental rights.[43]

At the heart of the legal dispute there was the possibility afforded by the Directive to let the national authorities obtain very intrusive and delicate information about many aspects of the private life of users of telecommunications service providers. This case is particularly important because it has highlighted the difference between the right to private life and the right to data protection and its autonomous regime as stressed by the Advocate General Cruz Villalòn's opinion.[44] In this sense, a restriction consistent with Article 7 of the Charter could not be compatible with the protection granted by Article 8 of the Charter, and vice versa. Moreover, an additional, innovative step was taken in the reasoning of the Court. Indeed, the balancing process was enriched off a scrutiny based on the provision of Article 52(1) of the Charter, specifically concerning, on one hand, a possible violation of the essence of the rights provided by Articles 7 and 8 of the Charter, and on the other hand, the respect of the principle of proportionality regarding the measures specified by the Directive to achieve the objectives of safeguarding public order and preventing terrorism, which are legitimate aims according to the court.[45]

Concerning the violation of the essence of rights, an infringement of the essence of both the right to privacy and the right to data protection was not found by the court. Consequently, in the first part of the balancing process, the aims sought by those measures, the prevention of terrorism, et cetera, allow a restriction of rights codified in Articles 7 and 8 of the Charter. However, it is in relation to the second profile of Article 52, the assessment of the proportionality of the collection and storage of data, that the court has found a breach of EU primary law. Under those aspects, the court has claimed that both the notion of "serious crimes"—too inaccurate and generic—and the lack of specific guarantees—from both a substantive and a procedural standpoint—regarding the actions of national authorities were incompatible with the principle of proportionality.[46]

Although this case involves a territorial use of data, the decision sets up the legal bases of the centripetal force of the EU right to data protection. Indeed, what is important in this decision is the high standard of the EU system in protecting fundamental rights of privacy and data protection and the beginning of a reconstruction of the super right to digital privacy. Additionally, the last innovative aspect of the decision is the use of the principle of proportionality. In this perspective, it could also be highlighted that by referring to the principle of proportionality as a "separate" element of the balancing process, the Court has

---

43 *Id.*

44 *Id.* ¶ 55.

45 *Id.* ¶¶ 54–55.

46 *Id.*

the possibility to both find new "infringements" of the super right to privacy online and to limit that right in order to not infringe the digital sovereignty of third states. However, in the ECJ's decisions, the second path seems to fall on deaf ears.

1. Building the Fortress in *Google Spain v. AEPD*

Member States have also taken different approaches as to how they intend to treat the nexus between personal data and freedom of expression. This is particularly relevant in light of the *Google Spain v. AEPD*[47] ruling of the ECJ in 2014.[48] In 2010, the plaintiff, Mario Costeja, requested that Google and La Vanguardia, a Spanish newspaper, remove his information from their sites regarding details of a government auction on his home for bankruptcy.[49] While the ultimate question in the case was whether an individual had the well-known right to be forgotten, the decision implicated freedom of information and expression since a news source was involved.[50] The rights to freedom of information and expression are protected in Article 10 of the European Convention on Human Rights but are subject to restrictions that are "in accordance with law" and "necessary in a democratic society."[51]

The right to erasure was upheld in the *Google Spain* decision despite the Advocate General's ("AG") opinion that this right created a tension with the more established right to freedom of expression.[52]

---

[47] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014).

[48] *Id.*

[49] Ignacio N. Cofone, *Google v. Spain: A Right to be Forgotten?*, 15 CHI.–KENT J. INT'L & COMP. L. 1, 3 (2015).

[50] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶ 80 (May 13, 2014).

[51] EUROPEAN CONVENTION ON HUMAN RIGHTS, art. 10(2), https://www.echr.coe.int/Documents/Convention_ENG.pdf. The same article also provides that such freedom also carries with it a responsibility to "[prevent] disclosure of information received in confidence" and that it may be restricted to protect the reputation or rights of others. *Id.*

[52] Opinion of Advocate General Jääskinen ¶ 2, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2013:424 (June 25, 2013).

> The particularly complex and difficult constellation of fundamental rights that this case presents prevents justification for reinforcing the data subjects' legal position under the Directive, and imbuing it with a right to be forgotten. This would entail sacrificing pivotal rights such as freedom of expression and information. I would also discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the Internet search engine service provider. Such "'"notice and take down procedures"',' if required by the Court, are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the

In this case, the court interpreted the relevant parameters aiming to give the widest possible protection to the rights to privacy and data protection. The litigation had its root in a Spanish proceeding, in which the domestic authority for the data protection ordered Google to remove some information from the results of the queries of the search engine.[53] Specifically, the removal concerned the links that resulted from the use of the plaintiff's name as a keyword. Indeed, the applicant appealed for removing from the Google results a piece of news published by a legal bulletin relating to a proceeding implicating him in something that happened many years before. Against this background, the American search engine rejected the request pointing out that a U.S.-based company was not subject to EU law and, therefore, to the Spanish law applying the data protection directive.

This was the first clash between the U.S. legal paradigm and the European one. The point of view expressed by Google was based on the balance of fundamental rights. Indeed, according to the U.S.-based search engine, an injunction like the one proposed under the Spanish law would have most likely restricted the freedom of expression of the website owners. This argument was founded both on the idea that search engines enjoy an autonomous right to free speech, but also that they are subject to a different approach in the protection of data in the U.S. legal regime.

The core of the case was—as stressed by Advocate General Jääskinen—the possible application of the individual's right to be forgotten against the Internet search engine service providers.[54] Taking into consideration the balancing process developed by ECJ judges, it can be stressed that the court claimed the existence of the right to be forgotten by providing it with some (maybe improper) legal basis. The court, in the balancing process, has sacrificed the freedom of information, contradicting the Jääskinen opinion that ranked the freedom of expression as a "primary right[]."[55] In doing that, the ECJ denied the right to free speech of search engines or web owners,[56] but above all, it has determined that a U.S.-based company is subject to EU law if it is operating in the EU. In this sense, it could be underlined how the court's data protection–

> most popular and important Internet search engine service providers. In this context it is necessary to recall that "notice and take down procedures" that appear in the ecommerce Directive 2000/31 relate to unlawful content, but in the context of the case at hand we are faced with a request for suppressing legitimate and legal information that has entered the public sphere.

Id.

53 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014).

54 *Id.*

55 *Id.*

56 One of the most evident anomalies in the reasoning of the Court is the lack of mention of Article 11 and Article 16 of the Charter, which respectively protect freedom of expression and freedom to conduct business.

oriented approach has led to a sort of chronological switch in the interpretation and reasoning concerning Article 7 and Article 8 of the Charter. The Articles of the Charter, enshrined at the beginning of 2000, were used to implement a precedential secondary law. In this perspective, the relevance of Articles 7 and 8 cannot be ignored as it has led and inspired the court in considering Google as a controller. Following from *Google Spain*, the court in *L'Oréal SA v. eBay International*[57] claimed:

> It follows from the foregoing that the answer to Question 1(a) is that Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State. [58]

In this case, it is evident how the extreme degree of protection granted to personal data on the Internet under Articles 7 and 8 involved the risk of an excess of Europeanization of Internet regulation, which contains two main issues. The first deals with the "physical" place where data is stored, and it is strictly linked to the problem of determining the applicable law on the Internet. The second concerns the attitude to apply EU law and the European paradigm of the right to data protection every time it comes to an individual resident of the EU.

Focusing on the first aspect, it can be stressed that this point has been anticipated in the *Digital Rights Ireland* decision in which the Court of Justice affirmed:

> [The] directive does not require the data in question to be retained within the European Union . . . it cannot be held that the control, explicitly required by Article 8, paragraph 3 of the Charter, by an independent authority of compliance with the requirements of protection and security . . . is fully ensured. [59]

From this perspective, *Google Spain* has been a further step toward the Europeanization of the protection of data on the Internet, consolidating the protection and field of application of EU law.

---

57 Case C-324/09, L'Oréal SA v. eBay Int'l AG, ECLI:EU:C:2010:757, ¶ 63 (Dec. 9, 2010).

58 *Id.*

59 Joined Cases C-293/12 and C-594/12 Digital Rts. Ir. Ltd. v. Minister for Commc'ns, ECLI:EU:C:2014:238, ¶ 68 (Apr. 8, 2014).

From the second point of view, in *Google Spain*, the ECJ considered the EU law applicable when the data of an EU resident are affected, regardless of where the servers processing the personal data are located. This is due to the large interpretation given to the expression "context of the activities" of an establishment, which allows the ECJ to apply a criterion very similar to the current GDPR Article 3(2) ("Territorial scope"). In this way, the court has created an *ante litteram* extraterritorial protection of the European right to data protection on the Internet.

Google Spain was the first complete attempt to build a fortress for the protection of personal data of individuals residing in Europe. This fortress was founded on two pillars: the European law and the EU "territory." The digital territory seems to be the most critical point of this reconstruction; the transnational nature of the Internet appears to be irreconcilable with the attempts of regionalization of the protection of data in the online environment.

The *Google Spain* judgment seemed inconsistent with various Member States' rules on personal data and freedom of expression. Ireland and France, for instance, both explicitly exempted GDPR application in instances where personal data was processed for "journalistic purposes."[60] This would presumably mean that the *Google Spain* decision becomes obsolete should another instance arise wherein an individual's personal information becomes implicated through dissemination by a news source.

Semantics become important for implementation in such areas, and ambiguous language can leave unanswered questions related to how personal data will be treated against an interest in freedom of expression. For instance, while the Irish and French rules lend immunity to news sources, Belgium's rules only declare "a large number of GDPR provisions [as] inapplicable or conditionally applicable to processing for journalistic purposes."[61] The language of the Belgian rule would therefore seemingly uphold the right to erasure in only certain instances that implicate freedom of expression, but not others. Additionally, the Belgian method of implementation does not answer the question of how it would identify instances where the right to erasure is to be upheld.

---

[60] Loi 2018-493 du 20 juin 2018 [Law 2018-493 of June 20, 2018 on Information Technology, Data Files and Civil Liberites] (Fr.); Irish Data Protection Act (Act No.7/2018), § 43(1), http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/pdf.

[61] *Belgium*, *GDPR Tracker*, BIRD & BIRD, https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker/belgium (last visited Sept. 6, 2020); Loi dui 5 septembre le comite instituant le comité de sécurité de l'information et modifiant devierseslois concernant la mise en œuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avirl 2015 [Law of Sept. 5, 2018 establishing the Information Security Committee and amending its laws concering the implementation of Regulation (EU) 2016/679 of the European Parliment and of the Council 27 April 2015], Moniteur Belge [M.B.] [Official Gazette of Belgium] (Sept. 10, 2018).

2. Judicial Pragmatism in *Schrems v. Data Protection Commissioner*

The second important step in what someone can consider as a sort of EU imperialism is *Schrems v. Data Protection Commissioner*"".[62] In this very famous decision, the court invalided the so-called safe harbor agreement, forcing the EU and the U.S. to renegotiate the conditions for an effective protection of personal data. Looking at the decision of the court, it can be underlined that following the manipulative approach adopted in the *Digital Rights Ireland* and *Google Spain* judgments, the EJC tried to extend up to the hilt of the protection of online data. The premise of this action is the nature of the fundamental right to data protection and the right to privacy.[63]

In this sense, the ECJ has analyzed and reviewed the consistency of the conditions of the Decision 2000/520 with the "adequate" level of protection for personal data to be transferred to third countries required by Article 25 of the Data Protection Directive. Thus, the EJC has reviewed if the U.S. legal system and the safe harbor principles guaranteed "an adequate level of protection" of the personal data of European residents. In doing this review, the Court applied a fundamental rights-based assessment looking at Article 7 and Article 8 of the Charter. In this sense, the Court has developed a sort of standard requiring equivalence in protecting personal data between the compared legal orders. Therefore, the ECJ extended the territorial coverage of the fundamental right to data protection by requiring a geographical extension of the guarantees provided for by EU law:

> The word "adequate" in Article 25(6) of Directive 95/46 admittedly signifies that a third country cannot be required to ensure a level of protection identical to that guaranteed in the EU legal order. However, as the Advocate General has observed in point 141 of his Opinion, the term "'adequate level of protection'" must be understood as requiring 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 by virtue of Directive 95/46 read in the light of the Charter. If there were no such requirement, the objective referred to in the previous paragraph of the present judgment would be disregarded. Furthermore, the high level of protection guaranteed by Directive 95/46 read in the light of the Charter could easily be circumvented by transfers of personal data from

---

62 Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650 (Oct. 6, 2015).

63 *Id.* ¶ 38.

> the European Union to third countries for the purpose of being processed in those countries.[64]

In conclusion, as stressed in *Google Spain*, the Charter, specifically Articles 7 and 8, becomes the trump card to make the protection required by EU law stronger and to extend the "territorial scope" of EU law in the online environment. This happens through a manipulation of the EU law, in this case, the parameter of "adequacy" of Article 25 of Directive 95/46. Additionally, the standard of adequacy shall not be seen only from a geographical point of view, but also over time.[65]

Thus, *Schrems* was another step toward a Europeanization of online data protection. Even though the court conceded that third party countries can develop their own solutions to grant "the adequate level of protection,"[66] this assumption has not led the court to adopt a self-restraint approach. Indeed, in reviewing if an adequate protection is actually met in the U.S. legal system, the ECJ has analyzed the actual and current legal tools in force in the U.S. and their consistency with the EU law. In doing that, the court has shown a pragmatic view, quite uncommon in the judicial review of fundamental rights. From this perspective, the absence of a fully recognized protection of data protection in the U.S. system has probably influenced the approach of the Court.

III. BEYOND EU CONVERGENCE

A. Decentralized Regulation

Although the GDPR is crafted from an EU-wide consensus on data privacy standards, each Member State is also given the opportunity to tailor the implementation process to its own preference.[67] The language of the GDPR allows for deviations by including the terms "may" and "shall" in certain provisions, such as those pertaining to national security and crime prevention.[68] While the permission of exceptions is important in maintaining the sovereignty of each EU Member State, such exceptions are also the root cause of variations in enforcement of the GDPR.

---

64 *Id.* ¶ 73.

65 This approach reflects the influence of the Advocate General's opinion, particularly at ¶¶ 146–48. *Id.*

66 *Id.* ¶ 6.

67 *See* GDPR, *supra* note 1.

68 *Id.* art. 6(1); *see also, e.g.*, *id.* § 45 ("This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing.").

1. The Commission's Role

The GDPR's allowance of deviations is a result of the Commission's role. Indeed, beyond the framework of data protection, in recent years, the Commission adopted not only hard regulation like the GDPR, but it has also relied on different co-regulatory and self-regulatory measures to address the challenges coming from new technologies and, more generally, the digital environment. This is evident when focusing on the set of High-Level Expert Groups ("HLEG") and codes of conduct and practices, especially those on hate speech online and disinformation. For instance, in April 2018, the Commission published its Communication on Disinformation,[69] promoting a "European approach" to tackle the phenomenon. The Commission's communication came from the work of the HLEG set up in January 2018 to develop the EU strategy for fighting disinformation. The HLEG laid out the groundwork by investigating possible lines of action,[70] providing the design of general and specific objectives to tackle forms of online speech which are not illegal in themselves, but that may nevertheless prove harmful for citizens and society at large. According to the European constitutional commitment to the protection of fundamental rights and freedoms, as enshrined in the EU Charter of Fundamental Rights and broadly fashioned along the long standing constitutional paradigm of the ECHR, the HLEG's report assumed that any intervention to fight disinformation should not impair or interfere with fundamental rights and freedoms at stake, chiefly, freedom of expression, freedom of the press and pluralistic values. Accordingly, the response to the multi-faceted nature of disinformation practices was the design of a "multidimensional approach" in order to adequately frame the complexity of the phenomenon, as well as to consider the diverse range of stakeholders involved.

Even in the field of hard regulation, this fragmentation can also be found in other legal measures.[71] For instance, the adoption of the Copyright Directive left broad margins of discretion to Member States in implementing its rules.[72] In particular, this choice introduces crucial issues, including issues concerning the exemption of liability of online platforms and the introduction of new safeguards regarding the platforms' processing of content according to Article 17. Likewise,

---

69 EUR. COMM'N, *Tackling Online Disinformation: A European Approach*, EUR–LEX (Apr. 26, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236.

70 EUR. COMM'N, A MULTI-DIMENSIONAL APPROACH TO DISINFORMATION, REPORT OF THE INDEPENDENT HIGH LEVEL GROUP ON FAKE NEWS AND ONLINE DISINFORMATION (2018).

71 Oreste Pollicino & Giovanni De Gregorio, *A Constitutional Change of Heart: ISP Liability and Artificial Intelligence in the Digital Single Market*, 18 GLOB. CMTY. Y.B. OF INT'L L. & JURIS. 237, 265–66 (2019).

72 Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April, 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96/9/EC and 2001/29/EC, ¶ 30–33, 2019 O.J. (L 130) 92.

the amendments to the Audio-Visual Media Service Directive reveals a similar pattern.[73] In this case, the framework is even more nuanced since the obligations introduced to video-sharing platforms are, in some cases, left to co-regulation, delegating competent authorities in Member States to adopt rules in sensitive fields like the safeguards to ensure the protection of minors and EU citizens from harmful content.[74]

Therefore, the GDPR is only the result of this framework. The broad margins of discretion or the lack of a normative language are the result of a common trend in the field of law and technology in the EU. Nevertheless, the degree of harmonization of data protection law in the EU increased thanks to the GDPR. Even if it is true that open clauses could undermine the goal of harmonization, the move from a Directive to a Regulation cannot be disregarded, not only from a formal standpoint, but also a substantive standpoint.

2. Conforming with the GDPR**:** Differentiated Approach in Germany and Italy

The German Data Protection Amendment Act ("GDPAA"), which updates Germany's previous data law to conform with the GDPR, takes liberties with the GDPR's flexible language in Article 9(2) regarding the use of "special categories of personal data."[75] The use of personal data is strictly prohibited if being used to "uniquely [identify] a natural person""; however, exceptions to this rule are allowed when necessary to carry out obligations and rights of the controller or to protect vital interests of the data subject.[76] The GDPAA makes use of these exceptions and allows the use of personal data for uses such as preventive medicine, employee capacity assessments, and medical diagnosis.[77]

Contrastingly, instead of creating a single rule regarding personal data, Italy's Legislative Decree note 101/2018 gives the "Garante" the responsibility of issuing provisions on safeguard measures for personal data every two years.[78]

---

[73] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November, 2018 Amending Directive 2010/13/EU on the Coordination of Certain Provisions Laid Down by Law, Regulation or Administrative Action in Member States Concerning the Provision of Audiovisual Media Services (Audiovisual Media Services Directive) in View of Changing Market Realities, ¶ 48, 2018 O.J. (L 303) 69.

[74] *Id.*

[75] GDPR, *supra* note 1, art. 9(1) (explaining that personal data includes health, biometrics, ideological, sexual, and genetic data).

[76] *Id.* art. 9(2)

[77] Lennart Schüßler & Natallia Karniyevich, *Germany Is the First EU Member State To Enact New Data Protection Act to Align with the GDPR*, BIRD & BIRD (July 2017), https://www.twobirds.com/en/news/articles/2017/germany/germany-is-the-first-eu-member-state-to-enact-new-data-protection-act-to-align-with-the-gdpr.

[78] Rocco Panetta, *Analysis: Italy's GDPR Implementation Law*, PRIV. TRACKER, https://iapp.org/news/a/analysis-italys-gdpr-implementation-law/ (last visited Sept. 13, 2020).

The benefits and drawbacks of the differences between the German and Italian methods of safeguarding personal health data will likely become apparent over time. Germany's standardization of its treatment may be beneficial in that it could be easier for consumers to understand and will not vary every few years. Whereas in Italy's case, the treatment of personal data will be updated every two years which could lead to confusion over how individuals' data is being treated with each determination issued by the Garante, while at the same time ensuring that laws will be more reactive to debates on data privacy and therefore more protective of individuals' data.[79]

3. Differentiated Enforcement

The differentiated enforcement of the GDPR leads to a variety of data privacy regimes in the EU. France is among the group of EU Member States that have decided to adopt a single bill for the implementation and adaptation of the GDPR and the Police Directive.[80] The New Personal Data Protection Act ("NDPA") implements the GDPR by creating new rights for the data subject, amends the current Loi No. 78-17 du 20 Juin 2018 governing personal data protection, and gives stronger enforcement mechanisms to La Commission Nationale de l'Informatique et des Libertés ("CNIL")—the French Data Protection Authority.[81] In conformity with the GDPR, the CNIL has the power to create guidelines and standards for data protection and is given strengthened investigation powers with regards to data centers and data controllers, which allows the CNIL to increase administrative fines and introduces penalties for obstructing the CNIL's operations.[82]

While the CNIL is being afforded greater liberties in enforcing the GDPR and protecting personal data, the Irish Office of the Data Protection Commissioner ("IDPC") is taking a more relaxed approach to GDPR compliance. Where the CNIL is given increased inspection powers with regard to data-retention centers, be it in data controller locations or elsewhere, the IDPC prefers negotiation to on-site inspections.[83] This is particularly troubling because a majority of the big tech companies that are governed by the GDPR are headquartered in Ireland, attracted by the more lenient regulations and tax

---

79 *Italy: Data Protection Law Integrating the GDPR in Place,* DLA PIPER (Sept. 10, 2018), https://blogs.dlapiper.com/privacymatters/italy-data-protection-law-integrating-the-gdpr-in-place/.

80 Transposition of the Directive (EU) 2016/680, EUR. UNION, http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=12946 (last visited Sept. 13, 2020).

81 NATIONAL ADAPTATIONS OF THE GDPR 52 (Karen McCullagh et al. eds., 2019).

82 *Id.* at 54–55.

83 Nicolas Vinocur, *How One Country Blocks the World on Data Privacy*, POLITICO (Apr. 29, 2019, 3:45 AM), https://www.politico.com/story/2019/04/24/ireland-data-privacy-1270123.

incentives.[84] Not only does this risk competition among EU Member States to have big tech companies headquartered within their jurisdiction, but it also allows those companies to escape stringent applications of the GDPR. Furthermore, Ireland has only recently announced that it intends to initiate a probe against Google for its data privacy practices related to online advertising.[85]

2018 saw implementation of the GDPR by EU Member States, and 2019 saw states initiating its enforcement. Member States are required to implement national penalties for breaches of the GDPR.[86] Where Ireland has only begun to explore penalties for violators of the GDPR, other states have instituted administrative penalties such as fines for breaches, and some have even gone so far as to create criminal offenses.[87] For instance, Spain's enforcement provisions are purely administrative at this stage.[88] Depending on the type of violation, maximum fines can range anywhere from €30,000 to millions of euros.[89] Spain penalizes the sending of marketing communications in breach of the GDPR with a maximum fine of €150,000 and penalizes breaches of applicable cookie restrictions with a fine of up to €30,000.[90] For repeat offenders who fail to comply with cookie restrictions, fines can reach up to €150,000 if a second violation is repeated "within three years after the first final decision of the Spanish Data Protection Agency"[91] Data security breaches induce even more expensive penalties, demanding administrative fines up to €10 million or alternatively, 2% of worldwide turnover from the previous financial year, applying the higher penalty.[92]

---

84 Edward Elmore, *Google Says It Will no Longer Use "Double Irish, Dutch Sandwich" Tax Loophole*, GUARDIAN (Jan. 1, 2020, 3:49 PM) https://www.theguardian.com/technology/2020/jan/01/google-says-it-will-no-longer-use-double-irish-dutch-sandwich-tax-loophole.

85 Ryan Browne, *EU Regulator Launches Probe into Google over Data Privacy*, CNBC (May 22, 2019, 1:00 PM), https://www.cnbc.com/2019/05/22/irish-data-privacy-watchdog-to-probe-google-over-potential-gdpr-breach.html.

86 Joanne Vengadesan & Katie Gordon, *United with Differences: Key GDPR Derogations Across Europe*, LEXOLOGY (Mar. 26, 2019), https://www.lexology.com/library/detail.aspx?g=9a9a3022-86bc-458e-b0e3-0cc24367a918.

87 *Id.*

88 *Id.*

89 Ruth Benito Martin & Alberto López Cazalilla, *Spain: Data Protection Laws and Regulations 2020*, ICLG (June 7, 2020), https://iclg.com/practice-areas/data-protection-laws-and-regulations/spain.

90 *Id.*

91 *Id.*

92 *Id.*

In June 2019, the Spanish Data Protection Agency enforced its GDPR compliance provisions against the Spanish professional soccer league, La Liga.[93] The league was fined €250,000 after being found guilty of abusing the transparency principles of the GDPR by using an app to remotely activate the microphone in a user's mobile device and listen in on them.[94] This was done to determine whether Spanish bars were showing football matches without paying the appropriate fees to stream them.[95] While the app did provide a warning to users that their personal data would be collected, the Spanish Data Protection Agency found it to be obscure.[96] Additionally, since the Agency viewed La Liga's use of the app as a method of personal data collection, it concluded that La Liga needed not only to explicitly notify the users that their data was being collected in such a way, but needed to do so every time that data collection occurred.[97]

La Liga has since argued that the fine is nothing more than a demonstration by the Spanish Data Protection Agency intended to exemplify its interpretation of the GDPR.[98] It also argues that the Agency's requirement that La Liga use a microphone icon to indicate its recording practices was not a foreseeable implication of the GDPR.[99] Considering that the same argument caused the Spanish National Court to rescind a fine of €150,000 which had been applied to Google, La Liga's argument may have some merit.[100] It is also noteworthy that the fine applied to La Liga for its personal data abuse is only a fraction of the GDPR's maximum penalty for these kinds of breaches, which can reach up to €20 billion or 4% of turnover.[101] Though this differs slightly from the Spanish limit of €10 billion or 2% turnover, the Spanish DPA will sometimes also apply the GDPR administrative fine if an infringement simultaneously

---

93 Juan Luis Sánchez & Carlos del Castillo, *The Data Protection Agency Fined LaLiga 250,000 Euros for the App that Uses the Microphone of Mobile Phones To Hunt Down Bars*, ELDIARIO (June 11, 2019, 12:43 PM), https://www.eldiario.es/tecnologia/Agencia-Proteccion-Datos-Liga-microfono_0_908859408.html.

94 Steve McCaskill, *La Liga Handed $280,000 GDPR Fine For "Spying" on Fans Watching Pirated Streams*, FORBES (June 12, 2019, 9:20 AM), https://www.forbes.com/sites/stevemccaskill/2019/06/12/la-liga-handed-e250000-gdpr-fine-for-spying-on-fans-watching-pirated-streams/#5b58602f75d9.

95 Sánchez & Castillo, *supra* note 93.

96 *Id.*

97 *Id.*

98 *Id.*

99 *Id.*

100 Carlos del Castillo, *The National Court Annuls the Fine of 150,000 Euros to Google for Notifying the Right To Be Forgotten to the Media*, ELDIARIO (May 27, 2019, 11:57 AM), https://www.eldiario.es/tecnologia/Audiencia-Nacional-Proteccion-Datos-Google_0_903610208.html.

101 McCaskill, *supra* note 94.

violates both the Spanish Law 34/2002 on information society services and ecommerce and the GDPR.[102]

The new German Bundesdatenschutzgesetz (BDSG), effective as of May 25, 2018, imposes imprisonment as a penalty for certain data protection infringements.[103] Instances where an individual's personal data is illegally transferred, made available on a large scale for commercial purposes, or fraudulently obtained for the purpose of enrichment can carry a penalty of up to three 'years imprisonment or a fine.[104] Thus far, Germany has been a leader in GDPR enforcement, being one of the first to begin compliance audits in July 2018.[105] As of early 2019, Germany has issued 41 fines for non-compliance with the GDPR.[106] The highest of these fines has been €80,000, issued to a business that allowed individuals' health data to be viewed by the public.[107] Even the highest penalty issued by the German Data Protection Authority so far is not remotely comparable to the giant €50 million fine issued by the CNIL against Google.[108] However, beyond an acknowledgment of a data breach against Airbus SE,[109] and a €400,000 fine against the real estate company Sergic,[110] it seems that France has been comparatively less thorough than Germany in enforcing GDPR compliance. While French penalties have been more expensive for non-compliant companies, German penalties have been more comprehensive. This would seem to solidify Germany's status as leader in GDPR compliance, which

---

102 Martin & Cazalilla, *supra* note 89.

103 Heinrich Amadeus Wolff, *The Implementation of Administrative Fines Under the General Data Protection Regulation from the German Perspective*, 2 INT'L J. DATA PROT. OFFICER, PRIV. OFFICER & PRIV. COUNS. 11, 13 (2018).

104 *Id.* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], June 30, 2017, BGBI I at 2097, last amended by Gesetz [G], Nov. 20, 2019, BGBI I at 1626, art. 12 (Ger.), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0338.

105 Susy Mendoza, *GDPR Compliance—It Takes a Village*, 42 SEATTLE U. L. REV. 1155 (2019); Focal Point Insights, *Get Ready: Germany's DPA's Are Starting Their GDPR Audits*, FOCAL POINT DATA RISK (Oct. 17, 2018), https://blog.focal-point.com/get-ready-germanys-dpas-are-starting-their-gdpr-audits.

106 Georgina Graham & Ashley Hurst, *GDPR Enforcement: How Are EU Regulators Flexing Their Muscles?*, IQ: THE RIM Q., Aug. 2019, at 20, 23.

107 Ray Schultz, *German Authorities Issue 41 GDPR Fines: Report*, MEDIAPOST (Feb. 25, 2019), https://www.mediapost.com/publications/article/332404/german-authorities-issue-41-gdpr-fines-report.html.

108 *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE L.L.C.*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

109 Benjamin D. Katz, *Airbus Hit by Cyber Breach. Says Aircraft Production Unaffected*, BLOOMBERG (Jan. 30, 2019), https://www.bloomberg.com/news/articles/2019-01-30/airbus-hit-by-cyber-breach-says-aircraft-production-unaffected.

110 *SERGIC: Sanction de 400,000€ pour Atteinte à la Sécurité des Données et Non-respect des Durées de Conservation*, CNIL (June 6, 2019), https://www.cnil.fr/fr/sergic-sanction-de-400-000eu-pour-atteinte-la-securite-des-donnees-et-non-respect-des-durees-de.

could indicate that other Member States may choose to follow in its footsteps—potentially implementing criminal provisions for non-compliance down the road.

B. The Polarity of the Territorial Scope in the ECJ Jurisprudence

Two decisions seem to have recently reversed the polarity of the territorial scope of the EU law: *Google L.L.C. v. Commission Nationale de l'Informatique et des Libertés ("CNIL")*[111] and *Glawischnig-Piesczek v. Facebook Ireland Ltd.*[112] Even if only one of these two decisions is strictly linked to the right to data protection, the two judgments shall be analyzed together because they seem to inaugurate a new trend in the approach to territorial scope of the EU law. If, on the one hand, *Google L.L.C.* 'seems to have stopped the progression of the territorial application of the EU law in the field of digital privacy, then *Glawischnig-Piesczek* seems to have opened the door to an eventual expansion of the EU balance between fundamental rights in the field of freedom of expression. This last field of action—even if this is not a harmonized matter under EU treaties—could be the new challenge for the coexistence of different digital sovereignties on the Internet.

1. *Google L.L.C. v. Commission Nationale de l'Informatique et des Libertés ("CNIL")*

In *Google v. CNIL*, the ECJ attempted to mitigate the most problematic systemic implications descendant from its ruling in *Google Spain*, limiting to the territory of Europe both the consequences of the "super" right to privacy, as formulated by *Google Spain,* and the range of application of EU law. The core of the decision is the nature of the right to be forgotten and its territorial scope: the single member state, the EU territory, or the whole world. From this point of view, two diametrically opposed solutions were proposed. The Google Advisory Council opted for a limitation of the right to be forgotten to the EU territory only,[113] while Working Party Article 29 proposed a global application of that right, not limiting it to European domains (e.g. ".es," ".eu," etc.).[114]

---

[111] Case C-507/17, Google L.L.C. v. Comm'n Nationale de l'Informatique et des Libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019).

[112] Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821 (Oct. 3, 2019).

[113] *The Advisory Council to Google on the Right To Be Forgotten* (Feb. 6, 2015), https://static.googleusercontent.com/media/archive.google.com/it//advisorycouncil/advisement/advisory-report.pdf.

[114] *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, EUR. COMM'N (Jan. 24, 2020), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236.

Starting from the conclusions of AG Macieji Szpunar, it has to be emphasized that a self-restraint approach is proposed, just as in the decision *Glawischnig-Piesczek*. AG Szpunar claimed that neither the EU law nor the ECJ case law faced the specific issue of the territoriality of the de-referencing in the protection of the rights of Articles 7 and 8,[115] *rectius* neither the EU rule-maker nor the EU judges dealt with the issue of how to treat and consider researchers infringing the right to be forgotten made out of the EU physical borders.

As a consequence, the main question was

> [i]f the provisions of Directive 95/46 are thus intended to protect the fundamental rights, on the basis of Articles 7 and 8 of the Charter, of the person "searched" and subsequently "referenced," they are silent, however, on the question of the territoriality of the de-referencing. By way of example, neither those provisions nor the judgment in *Google Spain v. AEPD* and *Google* make clear whether a search request made from Singapore must be treated differently from a search request made from Paris or from Katowice. [116]

The core of the AG's argument focused on the main reason behind the "digital imperialism" of the EU law and the ECJ jurisprudence with respect to the protection of fundamental rights online. From this point of view, admitting that in some fields it is possibly an extraterritorial effect, the AG's conclusions excluded the possibility of an expansion of the territorial scope of fundamental rights beyond the EU borders, both rejecting the argument of the extraterritorial effects of ECHR and excluding the nature of the super right not subjected to any balancing process of the right to be forgotten. Above all, this second element appears relevant, since the balance between fundamental rights is a territorial-based constitutional issue:

> If worldwide de-referencing were admitted, the EU authorities would not be in a position to define and determine a right to receive information, still less to strike a balance between that right and the other fundamental rights to data protection and to private life, *a fortiori* because such a public interest in having access to information will necessarily vary, depending on its geographic location, from one third State to another.[117]

The point raised by the AG concerns not only the problem of the "invasion" of other countries' sovereignty in designating their own balance

---

115 Opinion of Advocate General Szpunar, Case C-507/17, Google L.L.C. v. Comm'n Nationale de l'Informatique et des Libertés (CNIL), ECLI:EU:C:2019:15, ¶ 45 (Jan. 10, 2019).

116 *Id.*

117 *Id.* ¶ 60.

between fundamental rights, but also the increasing risk to determine a counteraction:

> If an authority within the European Union could order de-referencing on a worldwide scale, an inevitable signal would be sent to third countries, which could also order de-referencing under their own laws. Let us suppose that, for whatever reason, third countries interpret certain of their rights in such a way as to prevent persons located in a Member State of the European Union from having access to information which they sought. There would be a genuine risk of a race to the bottom, to the detriment of freedom of expression, on a European and worldwide scale.[118]

In conclusion, the proposal of the AG is that of the '"geo-'blocking" technology applied to the EU territory.

Against this background, the court, which once reaffirmed the application of the EU law at the activities of search engines and observed that the CNIL had refused the proposal of a "geo-blocking" application as formulated by Google, analyzed the questions proposed for a preliminary ruling: whether, according to Articles 12(b) and 14 of Directive 95/46 and Article 17(1) of Regulation 2016/679, the de-referencing is due on all the versions of the search engine, only on the versions of that search engine corresponding to all the Member States, or even only on the version corresponding to the Member State where the de-referencing has been required.

The global nature of the Internet—a global network without borders—and the claims of the right to digital privacy and data protection seemed to open the door to a new chapter of the extra-territoriality saga:

> Such considerations are such as to justify the existence of a competence on the part of the EU legislature to lay down the obligation, for a search engine operator, to carry out, when granting a request for de-referencing made by such a person, a de-referencing on all the versions of its search engine.[119]

However, the court—embracing the 'AG's opinion—highlights the different approach to the right to data protection and digital privacy in the different legal systems and the uncertain nature of this right. Two of the pillars at the foundation of the extraterritoriality effect seem to fall: on the one hand, it is recognized that there is the limited digital sovereignty of the EU law—or better, it is recognized that even in the digital, there are different sovereignties—and on the other hand, the trump card of the absolute right to data protection and

---

[118] *Id.* ¶ 61.

[119] Case C-507/17, Google L.L.C. v. Comm'n Nationale de l'Informatique et des Libertés (CNIL), ECLI:EU:C:2019:772, ¶ 58 (Sept. 24, 2019).

privacy online seems to be partially declined. As a consequence, even if the best solution for the ECJ would have been the global one, the court opted for self-restraint, motivated by the risk of a sort of European legal colonization led in the name of the cultural hegemony.

However, this decision seems more a tactical retreat than a surrender to the criticism against the Europeanization of the Internet regulation; it appears to be a self-restraint approach of the Judicial power waiting for the decision of the political one. The court has indeed affirmed

> [w]hile the EU legislature has, in Article 17(3)(a) of Regulation 2016/679, struck a balance between that right and that freedom so far as the Union is concerned (see, to that effect, today's judgment, *GC and Others (De-referencing of sensitive data*), C-136/17, paragraph 59), it must be found that, by contrast, it has not, to date, struck such a balance as regards the scope of a de-referencing outside the Union.[120]

Aside from these considerations, the obligation to remove contents infringing the right to privacy seems to be restricted to the EU Member States.[121] A certain "margin of appreciation" seems to be left to national authorities in demanding a global removal.

2. *Glawischnig-Piesczek v. Facebook Ireland Ltd.*

The second decision, *Glawischnig-Piesczek v. Facebook*, does not concern data protection and instead analyzes a disharmonized field.[122] However,

---

120 *Id.* ¶ 61.

121 *Id.* ¶ 66.

> [T]he EU legislature has now chosen to lay down the rules concerning data protection by way of a regulation, which is directly applicable in all the Member States, which has been done, as is emphasised by recital 10 of Regulation 2016/679, in order to ensure a consistent and high level of protection throughout the European Union and to remove the obstacles to flows of personal data within the Union, that the de-referencing in question is, in principle, supposed to be carried out in respect of all the Member States.

Id.

122 As stressed by the same AG,

> The situation at issue in the main proceedings is, prima facie, different from that which constituted the starting point of my analysis concerning the territorial scope of a de-referencing of the results of a search engine in *Google (Territorial scope of de-referencing)*, cited by Facebook Ireland and the Latvian Government. That case concerns Directive 95/46/EC, which harmonises, at Union level, certain material rules on data protection. It was, notably, the fact that the applicable material rules are harmonised that led me to conclude that a service provider had to be required to delete the results displayed following a search carried out not only from a single Member State but from a place within the European Union. However, in my Opinion in that

it is still quite useful to individuate a trend in the Europeanization of the territorial scope of EU law.

The EU has intervened in the free-speech field,[123] even if this matter is not fully harmonized because different balancing processes exist in Member States concerning the limits of freedom of expression. The willingness of EU institutions to create a *droit acquis communautaire* in the free speech field could stem from various factors that cannot be analyzed in this paper (e.g., helping the political integration of the EU, answering to the populist challenges, facing the crisis of European values and the rising of fair right parties and illiberal democracies, and fighting the foreign propaganda and influences). In this sense, EU action in the free speech field consists of two soft law tools: the Code of Conduct on countering illegal hate speech online,[124] aimed at censuring hate speech on Internet platforms, and the Code of Practice on disinformation, which enshrined the first attempt to regulate the giants of the web in the field of disinformation and misinformation.[125] Both the initiatives follow a broad work of expert groups, European Parliament resolutions, and even Member States' domestic legislation.

In this framework, it shall be stressed that as in the matter of digital privacy, the European balance of fundamental rights is quite different from the U.S. one.[126] As a consequence, another clash of digital sovereignties could

---

> case I did not exclude the possibility that there might be situations in which the interest of the Union requires the application of the provisions of that directive beyond the territory of the European Union.

Opinion of Advocate General Szpunar, Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:458, ¶ 79 (June 4, 2019).

[123] *See, e.g.*, Directive 2011/93/EU, of the European Parliament and of the Council of 13 December, 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography and Replacing Council Framework Decision 2004/68/JHA, 2011 O.J. (L 335) 1–14; Directive 2017/541, of the European Parliament and of the Council of 15 March, 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, 2017 O.J. (L 88) 6-21 (EU); Commission Recommendation 2018/334 of 1 March, 2018 on measures to effectively tackle illegal content online C/2018/1177, 2018 O.J. (L 63) 50-61 (EU); Commission Proposal for a Regulation of The European Parliament and of the Council of 9 December, 2018 on Preventing the Dissemination of Terrorist Content Online, COM (2018) 640 final.

[124] *The EU Code of Conduct on Countering Illegal Hate Speech Online*, EUR. COMM'N, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (last visited Sept. 6, 2020).

[125] *Code of Practice on Disinformation*, EUR. COMM'N (July 7, 2020), https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[126] If in the U.S. legal system, the doctrine of the marketplace of ideas shall consider state's intervention in the public discourse as inconsistent with First Amendment, the European scenario in the ECHR's case law has embraced a different balancing process of the limits of free speech. Under Article 10 of the ECHR and Article 11 of the Charter of Nice, not all forms of speech enjoy

deflagrate the Internet and feed the conflict between Internet regulation and the territorial scope of protection of fundamental rights. In this sense, it shall be stressed that, as opposed to digital privacy, the free speech matter lacks one of the two following elements: the super fundamental right or different concepts of that right. These elements have alimented the digital privacy issue, i.e., the presence of a super fundamental right, or better, an undisputed balance of fundamental rights in the matter of free speech. But by looking closer at EU policies, it is possible to highlight that, founding their legal basis on the ECHR case law, the Code of Conduct and the Code of Practice are working on this. These two tools are proposing a very clear idea of what the limits of freedom of speech should be, even if they are only slightly outlined in Article 11 of the EU Charter of fundamental rights and in ECJ case law.[127]

The decision in *Glawischnig-Piesczek* deals with the removal of defamatory content from Facebook under Directive 2000/31. The two main issues of the decision were the type of contents that can be removed and the range of application of EU law. In this Article, the issue of the removal of the identical allegations and/or "equivalent content" will not be explored under the key of the privatization of censorship. Instead, this Article will confine the analysis to the matter of the territorial application of EU law and focusing on the similarities to the other decisions in terms of territorial scope.

Briefly analyzing the first issue, the court chose not to limit the removal to identical contents but to allow the removal of equivalent contents, widening the content-based control over the information spread; this seems to be the first problematic profile linked to the decision. Allowing the removal of more content considered equivalent in its nature to the banned ones could increase the chances that a different balance of rights would have been assumed in a third country concerning the expression not covered by free speech clauses. For instance, the clash between the balancing processes is clearly evidenced by comparing the balance assumed by the Supreme Court of the Unites States in the defamatory cases[128] with the Austrian one.

Again, as in *Google v. CNIL*, the conclusions of AG Szpunar lean toward a geographically limited application of the national law even in the digital world. First of all, the problems of other state's digital sovereignty as linked to a general application of a national law is underlined:

---

the same regime of protection, and this is particularly evident in the fields of hate speech and fake news. *See* Oreste Pollicino & Eletra Bietti, *Truth and Deception Across the Atlantic: A Roadmap of Disinformation in the US and Europe*, 11 ITALIAN J. PUB. L. 57 (2019); Frederick Schaurer, *Freedom of Expression Adjudication in Europe and America: A Case Study in Comparative Constitutional Architecture* (Univ. Va. Sch. of L., Working Paper No. RWP05-019, 2005).

127 In this Section, the issue of the legitimation of this EU action, which could be disputed since this is not a harmonized or EU competence field, shall not be analyzed.

128 For more information about the *probatio diabolica* of the "actual malice" in the U.S. system, see Kyu Ho Youm, *"Actual Malice" in U.S. Defamation Law: The Minority of One Doctrine in the World?*, 4 J. INT'L ENT. & MEDIA L. 1 (2011).

> [A]s regards defamatory infringements, the imposition in one Member State of an obligation consisting in removing certain information worldwide, for all users of an electronic platform, because of the illegality of that information established under an applicable law, would have the consequence that the finding of its illegality would have effects in other States. In other words, the finding of the illegal nature of the information in question would extend to the territories of those other States. However, it is not precluded that, according to the laws designated as applicable under those States' national conflict rules, that information might be considered legal.[129]

Highlighting the inharmonious nature of the defamation law and the fact that no European provisions preclude an order of removal on a global-based scale, the AG hopes that

> in the interest of international comity . . . that court should, as far as possible, limit the extraterritorial effects of its junctions concerning harm to private life and personality rights. The implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. Thus, instead of removing the content, that court might, in an appropriate case, order that access to that information be disabled with the help of geo-blocking.[130]

Given the above, the court, as in *Google v. CNIL*, affirmed that no EU provisions impose a territorial limitation in that field. "However, it is apparent from recitals 58 and 60 of that directive that, in view of the global dimension of electronic commerce, the EU legislature considered it necessary to ensure that EU rules in that area are consistent with the rules applicable at international level."[131]

The decision of the court could be read as a green light to the national courts to impose a global scope to their decisions regarding the free speech issue.[132] Thus, the European Court in *Glawischnig-Piesczek* has not stopped the possibility of the extraterritorial effect of the EU Member States' laws. This approach, which is aimed at leaving an open-door policy regarding the extraterritorial scope of the EU law, could find new applications in the field of

---

[129] Opinion of Advocate General Szpunar, Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:458, ¶ 80 (June 4, 2019).

[130] *Id.* ¶ 100.

[131] Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821, ¶ 51 (Oct. 3, 2019).

[132] Pam Cowburn, *CJEU Judgment in Facebook Ireland Case Is Threat to Online Free Speech*, ARTICLE19 (Oct. 8, 2019), https://www.article19.org/resources/cjeu-judgment-in-facebook-ireland-case-is-threat-to-online-free-speech/.

fake news and hate speech, which are subjected to a high level of attention by the EU institutions.

It is perhaps possible, due to the growing convergence of the principles regulating content moderation and data protection,[133] to read this decision in a broader trend: the Europeanization of Internet regulation, regardless of its consequence on third countries' sovereignty.

Additionally, it must be stressed that a Sword of Damocles is hanging over this apparent self-restrained approach of the ECJ: the court seems to leave room for the political power to decide over the territorial scope of EU law. The court in these two decisions has not excluded the global territorial application of EU fundamental rights.

IV. U.S. SECTORAL PRIVACY REGULATION

A. Lack of an Overarching Federal Data Regulation

Data privacy regulation in the U.S. lacks an overarching federal mechanism by which data privacy is standardized. While states are free to craft their own privacy laws, the U.S. lacks a GDPR-like federal law to guide the creation of such state laws. Prompted by the Watergate scandal, the Privacy Act of 1974 was one of the first privacy tools crafted to manage the collection, maintenance, use, and dissemination of individuals' personal data obtained by federal agencies.[134] However, the Privacy Act solely governs the data stored by federal agencies, not businesses or other entities, which leaves individuals at the mercy of companies like Facebook and Amazon.[135] Similarly, the remaining U.S. privacy regulations are situation-specific, leaving a dearth of legal protection in the data privacy sphere.

The stipulations of the Privacy Act prevent federal agencies from disclosing private data to third parties without the consent of the individual in question, guarantee individuals' rights to access their own data retained by an agency, and allow requests for an amendment of information.[136] Civil remedies are available for alleged breaches of data use by agencies and include causes of actions such as wrongful denial of access to information retained by agencies, wrongful disclosure to third parties, and improper maintenance of records in accordance with requirements of the Privacy Act.[137] Civil liabilities for data misuse are also available under the Children's Online Privacy Protection Act of

---

133 Giovanni De Gregorio, *The E-Commerce Directive and GDPR: Towards Convergence of Legal Regimes in the Algorithmic Society?* (European Univ. Inst., Working Paper No. RSCAS 2019/36, 2019).

134 5 U.S.C.A. § 552a (West 2020).

135 *Id.*

136 *Id.* § 552a(b); *id.* § 552a(d)(1)–(2).

137 *Id.* § 552a(g)(1); *id.* § 552a(i)(1)–(3).

1974 ("COPPA").[138] COPPA recognizes the special state of childhood; it requires extra protection and appropriately forbids online service providers from collecting a child's data in any way that may conflict with regulations implemented by the FTC.[139] The Act creates a standard by which businesses are required to obtain parental consent before collecting private data on minors and to make their privacy policies easily accessible on their websites.[140]

The U.S. Congress has seen a few attempts from legislators to introduce broad federal regulations that would unify privacy standards across the nation.[141] Early 2018 saw the introduction of the Social Media Privacy Protection and Consumer Rights Act.[142] Though the bill was never passed, it proved to be an important starting point for federal privacy regulation proposals.[143] Senator Amy Klobuchar crafted the bill and introduced it just two weeks after Congress questioned Facebook CEO Mark Zuckerberg about the Cambridge Analytica Scandal of 2018, demonstrating that the proposed legislation was clearly a reactionary measure.[144] Under this proposed Act, online platform operators would have had the duty to inform users that their data would be collected and used by both the operator and third parties.[145] Platforms would have also been required to provide users with a copy of any data that was collected from them as well as information on how that data is used.[146] Any misuse of consumer data would need to be disclosed within a period of 72 hours after discovery.[147] The FTC would have been endowed with the responsibility of enforcing the bill under the Federal Trade Commission Act and the Communications Act of 1934.

Following the failure of the Social Media Privacy Protection and Consumer Rights Act to be passed into law, 15 Democratic senators introduced the Data Care Act of 2018, which also ultimately failed to pass.[148] The Data Care Act proposed a standard by which companies would have been required to protect consumer information and promptly notify consumers about data

---

138 15 U.S.C.A. § 6504(a)(1).

139 *Id.* § 6502(a).

140 *Id.* § 6502(b).

141 *See, e.g.*, Data Care Act of 2018, S. 3744, 115th Cong. (2018).

142 Social Media Privacy Protection and Consumer Rights Act of 2018, S. 2728, 115th Cong. (2018).

143 *Id.*

144 April Glaser, *There's a New Bill To Regulate Facebook and Google's Data Collection*, SLATE (Apr. 24, 2018), https://slate.com/technology/2018/04/the-new-bill-to-regulate-facebook-and-googles-data-might-actually-do-the-trick.html.

145 Social Media Privacy Protection and Consumer Rights Act of 2018, S. 2728, 115th Cong. (2018).

146 *Id.*

147 *Id.*

148 Data Care Act of 2018, S. 3744, 115th Cong. (2018).

breaches involving sensitive data, to not use identifying data in a way that would result in "reasonably foreseeable and material physical or financial harm to an end user," and to ensure the same standard for third-party businesses that were sold access to user information.[149] In comparison to its predecessor, the Data Care Act would have given the FTC not only the responsibility of enforcing the bill, but also of imposing civil penalties.[150] The bill also went further than Senator Klobuchar's proposition by specifying the types of data that would be protected, such as a user's social security number, driver's license number, biometric data, name, and birth data.[151]

The failure of the Data Care Act was followed by the introduction of the American Data Dissemination Act ("ADD Act") by Senator Marco Rubio.[152] The ADD Act's most unique feature in comparison to previous attempts at national privacy legislation was that this Act puts even more pressure on the FTC to be the overseer of all privacy infractions committed by companies.[153] The proposal gave the FTC a 180-day window within which to submit "detailed recommendations for privacy requirements that congress could impose on covered providers that would be substantially similar . . . to the . . . Privacy Act of 1974," which currently regulates government data collection.[154] After receipt of the FTC's recommendations, Congress would be allowed a two-year period by which it would need to enact privacy requirements for "covered providers" that are "substantially similar" to the requirements imposed on government agencies by the Privacy Act.[155] However, if Congress fails to appropriately respond within that two-year period, the burden again would fall on the FTC to enact final regulations that impose privacy requirements in accordance with the guidelines provided by the bill.[156]

The ADD Act takes note of the GDPR's effects, for instance, recognizing that the GDPR's provisions have been difficult for small businesses to implement and exempting them from a newly imposed federal privacy regulation.[157] Other general guidelines follow the same pattern as previous bills by restricting disclosure of consumer information and giving users the right to access records with their information and the right to request removal of

---

149 Kris Holt*, Senate Democrats Introduce Bill To Protect Your Online Data*, ENGADGET (Dec. 12, 2018), https://www.engadget.com/2018-12-12-senate-data-protection-bill-data-care-act.html.

150 Data Care Act of 2018, S. 3744, 115th Cong. (2018).

151 *Id.*

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

153 *Id.*

154 *Id.* (referring to big business Internet service providers as "covered providers").

155 *Id.*

156 *Id.*

157 Will Rinehart, *Understanding the ADD Act*, AM. ACTION F. (Jan. 17, 2019), https://www.americanactionforum.org/insight/understanding-the-add-act/.

information.[158] Though the ADD Act takes into consideration the pitfalls of the GDPR that businesses have experienced, it may still have unforeseen consequences. Many state regulations[159] make the mistake of focusing on data collection rather than data use, neglecting the source of harm to consumers, which is data misuse.[160]

Not only has federal legislation lacked a comprehensive individual approach to data privacy regulation for individuals, but most importantly the Communications Decency Act ("CDA") of 1996 was one of the earliest attempts in the U.S. to moderate free speech on the Internet by offering a shield from tort liability to online platforms.[161] The potential for end users on Internet service sites to violate libel or other restricted speech laws raised a question of whether Internet Service Providers ("ISPs") should be held liable for all of the content on their sites.[162] Judicial decisions on the issue assessed the responsibility of the ISPs to remove harmful or libelous content based on their knowledge and control over that content.[163] In a 1991 case, *Cubby, Inc. v. CompuServe, Inc.*,[164] the Southern District of New York found that an ISP could not be held liable for content that end users posted to its site if it did not regularly review such content as a business practice.[165] Lack of knowledge regarding the libelous content precluded liability for the ISP.[166] However, four years later in *Stratton Oakmont, Inc. v. Prodigy Services Co.*,[167] the Supreme Court of New York ("SCNY") reached a conclusion that relied on similar principles of ISP knowledge of harmful content, but used those principles to hold Prodigy Services Company responsible for content moderation on its site.[168]

The *Stratton Oakmont* decision, if left on its own, would have created a highly stringent standard for ISP tort liability. Prodigy Services Company ("Prodigy") was a widely utilized ISP whose business consisted wholly of

---

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

159 Lothar Determann & Helena J. Engfeldt, *Maine and Nevada's New Data Privacy Laws and the California Consumer Privacy Act Compared*, BAKER MCKENZIE (June 20, 2019), https://www.bakermckenzie.com/en/insight/publications/2019/06/maine-and-nevada-new-data-privacy-laws (explaining the provisions of Maine's Act to Protect the Privacy of Online Customer Information and its focus on data collection as opposed to data use).

160 Rinehart, *supra* note 157.

161 47 U.S.C.A. § 230 (West 2020).

162 *See generally* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

163 *Id.*

164 *Id.*

165 *Id.* at 143.

166 *Id.* at 139.

167 No. 31063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995).

168 *Id.* at *7.

message boards where users could post their thoughts without hinderance.[169] There was no initial filtration system that placed any form of restriction on what end users could post, but when Prodigy began to moderate its site content by removing certain messages for "bad taste" or being "grossly repugnant to community standards," the court seized the action as an opportunity to hold ISPs liable for the entirety of the content on their sites.[170] The resulting decision proposed to force ISPs to take a completely hands-off approach to content moderation in order to escape tort liability.

B. The Centrality of the First Amendment

In response to *Stratton Oakmont*, Congress recognized the negative effect that the SCNY's decision would have on innovation and users' First Amendment right to free speech. The CDA Section 230(c)(1) precludes ISPs from tort liability and states that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[171] In other words, Section 230(c)(1) has allowed ISPs to function without fear of being reprimanded for the content posted by end users, which could ultimately interfere with their entire business model. The protection is limited by the caveat that if the ISP has helped create content that enables criminal activity, safe harbor does not apply.[172] The CDA was challenged the year after it went into effect, and part of it was struck down by the Supreme Court for violating the First and Fifth Amendments of the United States Constitution. In *Reno v. ACLU*,[173] the CDA's general prohibition on "indecent communications" was deemed to be unconstitutional because it did not adequately distinguish between "indecent" versus "obscene" sexual expressions as the First Amendment does, making the restriction overly broad.[174] The First Amendment protects "indecent" speech, and therefore the CDA clause restricting such speech was unconstitutional.[175]

Since the *Reno* decision, CDA Section 230 has given ISPs broad immunity against tort claims. In 2003, Christine Carafano brought a private claim against Matchmaker.com, claiming that a false profile was made in her name that included her photos and resulted in her harassment by individuals who received her contact information from the account.[176] The injured party received sexually

---

169 *Id.* at *2.

170 *Id.*

171 47 U.S.C.A. § 230(c)(1) (West 2020).

172 Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1839 (2010).

173 521 U.S. 844 (1997).

174 *Id.* at 883.

175 *Id.* at 874.

176 Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003).

explicit text messages, phone calls, and e-mails as well as threats toward her and her son.[177] Carafano alleged "invasion of privacy, misappropriation of the right of publicity, defamation, and negligence."[178] Matchmaker.com was given complete immunity from the claim both in the lower and appellate court under Section 230.[179] The court found that Matchmaker.com was not responsible for the injury because while it provided a platform on which the profile could be created and even aided users in creating profiles with a questionnaire, it had not played a role in "creating, developing, or transforming the relevant information."[180]

In a similar decision, the Court of Appeals for the Ninth Circuit again upheld CDA Section 230 immunity for ISPs. The plaintiff in *Barnes v. Yahoo!, Inc.*[181] sued the ISP under a theory of negligent undertaking after it refused to remove indecent content depicting her, which her boyfriend posted on the site.[182] The protections under Section 230 effectively barred the plaintiff's complaints because it "precludes courts from treating Internet service providers as publishers not just for the purposes of defamation law . . . but in general."[183] The decision solidified the ''court's position that ISPs could not be held liable even in instances where speech violated other laws, such as defamation law.[184]

Section 230's preservation of online platforms' right to free speech is illustrative of the deference that American legislators give to the First Amendment over consumer protection interests. Until the middle of 2018, it was perfectly legal for the government to obtain cell-site location information ("CSLI") from wireless carriers to be used as evidence against a defendant in a criminal case. In the landmark decision *Carpenter v. United States*,[185] the Supreme Court held that the government would no longer be permitted to do this without a warrant under the Fourth Amendment.[186] The U.S. Constitution provides that the people have a right to "be secure in their persons, houses, papers, and effects against unreasonable searches and seizures."[187] The Court had also previously ruled that, for the purposes of the Fourth Amendment, GPS tracking of a vehicle also amounted to an unreasonable search.[188] The use of

---

177 *Id.*

178 *Id.* at 1122.

179 *Id.*at 1125.

180 *Id.*

181 570 F.3d 1096 (9th Cir. 2009).

182 *Id.* at 1099.

183 *Id.* at 1104.

184 *Id.*

185 138 S. Ct. 2206 (2018).

186 *Id.*

187 U.S. CONST. amend. IV.

188 United States v. Jones, 565 U.S. 400, 412–13 (2012).

CSLI by the government is akin to tracking a person's past movements over a prolonged period of time, as is placing a GPS tracker on a car.[189] Therefore, the government's arguments that the use of CSLI was constitutional because it was obtained from a third party and protected under the Stored Communications Act,[190] were found to be implausible under the Fourth Amendment.[191] The Court concluded that if the government wanted to obtain CSLI data, it first needed to obtain a warrant.[192]

However, *Carpenter* does nothing for private use of CSLI, making a federal privacy regulation all the more necessary. Wireless carriers are still participating in the sale of individuals' CSLI to third parties.[193] While *Carpenter* specifically restricts the government's use of prolonged tracking information, there is no law in place to prevent the government from hiring a third party with access to CSLI to track down an individual.[194] Similarly, bail bondsmen and related businesses, such as bounty hunters, have been found to have purchased CSLI from big wireless carriers to carry out their business objectives.[195]

C. U.S. Litigation on Consumer Privacy

The high-profile Cambridge Analytica scandal[196] involving social media giant Facebook raised public concern in the U.S. and the U.K. over how personal data was being used by tech companies. An estimated 87 million Facebook profiles were mined for data that was later sold to the political data-analysis firm Cambridge Analytica and was used to spread propaganda connected to the 2016 Trump campaign.[197] Individuals' profiles were used to not only gain access to

---

189 *Carpenter*, 138 S. Ct. at 2209.

190 18 U.S.C.A. § 2703(d) (West 2020), *invalidated in part by Carpenter*, 138 S. Ct. at 2210–11.

191 *Carpenter*, 138 S. Ct. at 2221.

192 *Id.*

193 SUSAN DENTE ROSS, AMY REYNOLDS & ROBERT TRAGER, THE LAW OF JOURNALISM AND MASS COMMUNICATION 249–50 (6th ed. 2019).

194 *Id.*

195 Joseph Cox, *Big Telecom Sold Highly Sensitive Customer GPS Data Typically Used for 911 Calls*, VICE (Feb. 6, 2019, 5:11 PM), https://www.vice.com/en_us/article/a3b3dg/big-telecom-sold-customer-gps-data-911-calls.

196 Nicholas Iovino, *Facebook Fights Multibillion-Dollar Privacy Class Action*, COURTHOUSE NEWS SERV. (Feb. 1, 2019), https://www.courthousenews.com/facebook-fights-multibillion-dollar-privacy-class-action/.

197 Ikhlaq ur Rehman, *Facebook-Cambridge Analytica Data Harvesting: What You Need To Know*, 2019 LIBR. PHIL. & PRAC. 7 (2019).

their personal data, but also to their friends' data.[198] Based on this data, users were subjected to target messaging that influenced the outcome of the Trump campaign, Brexit, and Kenya's presidential election.[199] The situation led to a massive class-action lawsuit in which the chief complaint[200] was that Facebook "improperly and without authorization" accessed and obtained users' personal information in violation of a consent decree that had been levied against the company in 2011 by the FTC.[201]

The class action suit resulting from the Cambridge Analytica breach was brought under the "hacking" statute of the Stored Communications Act.[202] That statute states that "whoever . . . knowingly and with intent to defraud accesses a protected computer without authorization or exceeds authorized access" will bear the assigned punishment in Subsection (c) of its provisions.[203] A single violation under the statute could yield a fine of up to $1,000, adding up to a maximum, but unlikely, amount of $70 billion as a penalty for improper privacy practices.[204] Facebook denied that it ever gave approval or had any formal knowledge regarding the misuse of user data alleged in the class action.[205]

The company's denial of liability went so far as to prompt it to file a motion to dismiss the class action complaint.[206] Facebook claimed that none of the members of the class who filed the complaint had suffered any harm, calling the bases for the complaint "bizarre" and "ranging from drained cell phone batteries to the election of President Trump."[207] The motion also relied on users' consent to third-party apps and targeted advertising as a defense to its

---

198 Jim Isaak & Mina J. Hanna, *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection*, IEEE COMPUT. SOC'Y (Aug. 2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400&tag=1.

199 *Id.*

200 Class Action Complaint at 2, Redmond v. Facebook, Inc., No. 3:18-CV-03642, 2018 WL 7047281 (N.D. Cal. Apr. 10, 2018).

201 Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, United States v. Facebook, Inc., No. 1:19-cv-02184 (D.D.C. July 24, 2019).

202 18 U.S.C.A. § 1030 (West 2020).

203 *Id.*

204 Owen Bowcott & Alex Hern, *Facebook and Cambridge Analytica Face Class Action Lawsuit*, GUARDIAN (Apr. 10, 2018), https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.

205 Kalev Leetaru, *The Problem Isn't Cambridge Analytica: It's Facebook*, FORBES (Mar. 19, 2018), https://www.forbes.com/sites/kalevleetaru/2018/03/19/the-problem-isnt-cambridge-analytica-its-facebook/#545ea3f058a5.

206 Memorandum of Law in Support of Motion of Defendant Facebook, Inc. to Dismiss Plaintiffs' Consolidated Complaint, *In re* Facebook, Inc., No. 3:18-MD-02843-VC (N.D. Cal. Jan. 23, 2019).

207 *Id.*

questionable privacy practices.[208] When the controversy led to questions over whether Facebook violated its 2011 consent decree, similar denials were offered in a statement released by the company: "We reject any suggestion of violation of the consent decree. We respected the privacy settings that people had in place. Privacy and data protections are fundamental to every decision we make."[209]

1. FTC Regulation of Facebook

The FTC consent decree bound Facebook to have a "comprehensive privacy program" and "obtain express consent" from users before sharing their data.[210] Not only did the Cambridge Analytica incident bring Facebook's compliance with the consent decree into question, but subsequent reports that the company had arranged to share data with more than 150 companies also brought further scrutiny.[211] Where Facebook's denial that it had any knowledge of Cambridge Analytica's abuse of user data may have had the possibility of acting as a sound defense against the class action suit, the same cannot not have been said regarding its agreements with these 150 third-party companies. These companies were permitted to abuse and manipulate user data when Facebook gave them permission to "read, write, and delete users' private messages."[212] In defense of its behavior, Facebook attempted to explain away the allegations it faced over these 150 "integration partnerships" by reasoning that they were created "so people [could] use Facebook on devices and platforms that" the company's service did not itself support.[213]

However, Facebook's statement failed to address the fact that users were unaware of how much of their data was being provided to these "partners."[214] Facebook also neglected to address the fact that users were often unaware that their data was being shared at all with third-party services.[215] The FTC found that

---

208 *Id.*

209 Craig Timberg & Tony Romm, *U.S. and British Lawmakers Demand Answers from Facebook Chief Executive Mark Zuckerberg*, WASH. POST (Mar. 18, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/18/u-s-and-british-lawmakers-demand-answers-from-facebook-chief-executive-mark-zuckerberg/.

210 Plaintiff's Consent Motion for Entry of Stipulated Order for Civil Penalty, Monetary Judgment, and Injunctive Relief, *supra* note 201, at 3–6.

211 Gabriel J.X. Dance, Michael LaForgia & Nicholas Confessore, *As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants*, N.Y. TIMES (Dec. 18, 2018), https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html.

212 Alex Johnson, *Facebook Denies It Let More Than 150 Companies Misuse Personal Data*, NBC NEWS (Dec. 18, 2018), https://www.nbcnews.com/tech/social-media/facebook-denies-it-let-other-tech-companies-misuse-personal-data-n949701.

213 *Id.*

214 *Id.*

215 *Id.*

these behaviors violated the FTC Act and an FTC order that Facebook had agreed to in 2012.[216] Under the 2012 order, Facebook was required to honor users' privacy settings and choices or face litigation from the FTC.[217] One of the complaints that prompted the 2012 order involved users' freedom to choose settings that allowed only their friends to access their information being negated by Facebook's failure to disclose that the same information could be accessed by third parties whose apps users' friends had installed.[218] Investigations revealed that even when users selected the most restrictive privacy settings, Facebook's business practices still made users' personal data available to companies that developed apps used by consumers' friends.[219]

The FTC's 2012 complaint also stated that Facebook's policy statement regarding its use of facial recognition technology was misrepresented to consumers.[220] The policy indicated that users would be automatically provided with "tag suggestions" for photos only when users had facial recognition settings turned on. When in reality, facial recognition was a default setting for all users.[221] The language of the policy suggested that users would only be provided with suggestions based on facial recognition if they opted in to the setting, but they actually needed to opt out to protect their data from being used.[222] Users were further duped into providing the company with their personal phone numbers under the guise of account recovery and security, but they were not informed that their numbers would also be used to serve them with targeted ads.[223]

These complaints amassed to a record penalty of $5 billion against Facebook for the aforementioned infractions.[224] Mark Zuckerberg, CEO of Facebook, has been heavily criticized for his company's lax data-privacy policies and has even faced attempts by Facebook shareholders to hold him personally liable to the company for breach of fiduciary duty.[225] The penalty assigned by the FTC also requires that Facebook implement measures to keep Zuckerberg's power as CEO in check. The company's Board of Directors will be required to

---

216 Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FTC BUS. BLOG, (July 24, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

217 *Id.*

218 *Id.*

219 *Id.*

220 *Id.*

221 *Id.*

222 *Id.*

223 *Id.*

224 *Id.*

225 Karl Baker, *Lawsuit Against Facebook Leaders Claims Zuckerberg Is Liable for Billion-Dollar Fine*, DEL. ONLINE (May 2, 2019), https://www.delawareonline.com/story/money/business/2019/05/02/latest-facebook-lawsuit-delaware-claims-zuckerberg-committed-insider-trading/3640123002/.

create an independent privacy committee from which Facebook officers and employees are excluded.[226] The site's policies will also be amended to more closely monitor third-party developers and refuse data access to any developer that is non-compliant with the new policies.[227]

On the same day that it was dealt the $5 billion fine, Facebook also publicly acknowledged that the FTC opened an antitrust investigation to the sprawling social media landscape that is becoming the company's empire.[228] Google and Amazon are also included in the investigation[229] as their influence raises similar antitrust concerns as Facebook's acquisition of smaller businesses like Instagram and Whatsapp.[230]

2. Attorney General Racine's Lawsuit Against Facebook

Not only did the Cambridge Analytica scandal prompt federal litigation against Facebook, but it also provoked a complaint from the Attorney General of the District of Columbia, Karl Racine.[231] Facebook is suspected to have had knowledge of the data mining carried out by Cambridge Analytica and allowed harm to befall consumers.[232] The complaint alleges that Facebook violated the D.C. Consumer Protection Procedures Act by deceiving users, neglecting to properly monitor third-party apps, and using confusing language in its privacy policy.[233] Additionally, it is widely known that Facebook took more than two years to disclose the details of the scandal to its consumers and the public, and to this, Attorney General Racine argues that it had a duty to promptly notify consumers of the breach.[234] The motive behind the lawsuit is to "[make]

---

226 Fair, *supra* note 216.

227 *Id.*

228 Steven Overly, *Facebook Discloses FTC Antitrust Investigation Underway*, POLITICO (July 14, 2019, 6:17 PM), https://www.politico.com/story/2019/07/24/facebook-discloses-ftc-antitrust-investigation-underway-1432927.

229 *Id.*

230 Mark Glick & Catherine Ruetschlin, *Big Tech Acquisitions and the Potential Competition Doctrine: The Case of Facebook* 3–5 (Inst. for New Econ. Thinking, Working Paper No. 104, 2019), https://www.ineteconomics.org/uploads/papers/WP-104-Glick-and-Reut-Oct-10.pdf.

231 Complaint for Violations of the Consumer Protection Procedures Act, District of Columbia v. Facebook, Inc., No. 2018-CA-008715-B (D.C. Super. Ct. Nov. 19, 2019) [hereinafter Complaint for Violations].

232 Hilary Tuttle, *Facebook Scandal Raises Data Privacy Concerns*, 65 RISK MGMT. 6, 8–9 (2018) ("[Facebook] knew a third party was collecting user data.").

233 Complaint for Violations, *supra* note 231, at 3.

234 *AG Racine Sues Facebook for Failing To Protect Millions of Users' Data*, OFF. OF THE ATT'Y GEN. FOR D.C. (Dec. 19, 2018), https://oag.dc.gov/release/ag-racine-sues-facebook-failing-protect-millions.

Facebook live up to its promise to protect its users' privacy."[235] The complaint aims to have an injunction granted against Facebook to ensure that the appropriate privacy safeguards are put in place as well as to encourage prompt action that allows users to more effectively control their privacy settings on the site.[236] ''Facebook's attorneys have made multiple attempts to have the complaints dismissed, but D.C. Superior Court Judge Fern Saddler has not been persuaded by their arguments that the case is not properly before the court and that the action will not prove that there was company misconduct.[237]

3. Balkanization of State Privacy Regulations

Various states within the U.S. are choosing to enact their own privacy regulations in the absence of a federal privacy law. For example, the State of Washington has modelled its legislation by following the GDPR. The Washington Privacy Act ("WPA") introduced in early 2019 proposed a new standard for privacy in the state that closely mirrored various provisions of the GDPR.[238] Both instruments employed similar tactics for protecting privacy and defined "personal data" as "any information relating to an identified or identifiable natural person."[239] The WPA also drew substantially on the protections provided in the GDPR, providing rights such as the right to be informed about what personal data is being collected, how it is used, and whether it is sold, as well as the right to receive a copy of personal data being kept by a data controller.[240] The WPA cited various motivations for its regulations ranging from constitutional protections to recent events such as data breaches involving tech companies.[241] The Act aimed to strike a balance between protecting innovation and economic growth for businesses while also reinstituting consumer confidence in those businesses when it comes to how their data is being handled.[242] The right to privacy protected in Article 1, Section 7 of the Washington Constitution and the Fourth Amendment of the U.S. Constitution were relied on as the source of inviolable consumer rights that inspired the creation of the WPA.[243] The text of the Act also specifically assigned

---

235 *Id.*

236 *Id.*

237 Andrew M. Harris & Daniel Stoller, *Facebook Is Accused of Knowing Cambridge Mined Its User Data*, BLOOMBERG (Mar. 22, 2019), https://www.bloomberg.com/news/articles/2019-03-22/facebook-fights-for-dismissal-of-d-c-privacy-protection-suit.

238 S.B. 5376, 66th Leg., Reg. Sess. (Wash. 2019).

239 *Id.* § 3.

240 *Id.* § 6.

241 *Id.* § 2.

242 *Id.*

243 *Id.*

responsibility to technology businesses for the recent "chilling of consumer confidence" and "cost [to] Washington state businesses."[244] While the Act found support in the state Senate, it was later quashed in the state House.[245] Had it succeeded at the state legislature, the WPA would have been the second state privacy regulation to be established in the U.S. after the CCPA.[246]

One major issue with the WPA was its approach to the regulation of facial recognition technology.[247] Section 14 of the Act proposed that data controllers obtain consent from consumers before making use of facial recognition services and provide conspicuous notice to consumers regarding the instances in which facial recognition technology would make use of their data.[248] Some critics argued that the regulation did not take enough action and that a moratorium should be placed on the technology instead.[249] The one major way that the WPA differed from the GDPR and CCPA was its failure to provide a private right of action for data misuse.[250] Therefore, while it purported to restore consumer confidence in technology, it did not, even at a minimum, provide a way for consumers to challenge businesses using their data in the event that the WPA failed to provide adequate protection.

In contrast, the proposed New York Privacy Act ("NYPA") does provide a private right of action for consumers, mirroring the provisions of the GDPR.[251] Consumers would have been enabled to sue companies directly for data breaches and other infractions involving data misuse. It also would have implemented GDPR-like transparency provisions which required companies to disclose to consumers how their data was being used, the purpose for its collection, and when and how data was shared with third parties.[252] Unlike the CCPA, which aims to mitigate compliance costs for smaller tech businesses, the NYPA took after the GDPR in indiscriminately applying its provisions to all businesses that collect consumer data, regardless of size.[253] The provisions were applied so

---

244 *Id.*

245 Lucas Ropek, *Why Did Washington State's Privacy Legislation Collapse?*, GOV'T TECH. (Apr. 19, 2019), https://www.govtech.com/policy/Why-Did-Washington-States-Privacy-Legislation-Collapse.html.

246 *Id.*

247 *Id.*

248 S.B. 5376, 66th Leg., 2020 Reg. Sess., § 3 (Wash. 2019).

249 Ropek, *supra* note 245.

250 *Id.*

251 S.B. 5642, 243 Leg. Sess. (N.Y. 2019).

252 Lucas Ropek, *NY's Data Privacy Bill Failed; Is There Hope Next Session?*, GOV'T TECH. (July 15, 2019), https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html.

253 Kevin Bampoe, *Landmark Data Privacy Legislation Serves as a Benchmark in a Rapidly Shifting Legal Landscape*, SYRACUSE J. SCI. & TECH. L. (Sept. 9, 2019),

broadly that even nonprofit institutions would have been affected by its passage.[254] This is a particular concern held by critics of state privacy regulations who fear that compliance costs could cause smaller start-up business who do not have adequate financial resources for compliance to fail as a result of laws like the NYPA.[255]

The NYPA's imposition of a fiduciary duty on businesses also caused concern among critics by shifting the burden of data protection on businesses instead of placing it on consumers by giving them a say in how their data is handled.[256] This would have required businesses to take on a role more akin to that of healthcare providers, who are prohibited from selling data to pharmaceutical companies.[257] These concerns, coupled with the criticism that the NYPA's passage would create an even stricter state privacy regulation than the CCPA, caused the NYPA to ultimately fail to pass into law at the state legislature.[258] It is likely that the inspiration behind the creation of a fiduciary duty came from Facebook's misleading data privacy language which duped consumers into providing their personal information for marketing purposes under the guise of protection.[259] Since giant tech companies like Facebook have become so integrated into consumers' lives, they have left consumers with no choice besides sharing their personal information. It makes sense that businesses should then have a responsibility to carefully handle sensitive data.[260]

The Massachusetts Act Relative to Consumer Data Privacy updates the data breach laws that the state previously had in place and brings the law closer to the GDPR standard for data protection.[261] Like the NYPA, the proposed Massachusetts law provides a right of action and does not require the plaintiff to have suffered a financial or material harm in order to file a claim.[262] As with

---

https://jost.syr.edu/landmark-data-privacy-legislation-serves-as-a-benchmark-in-a-rapidly-shifting-legal-landscape/.

254 Philip Yannella, *New York State Data Privacy Law Fails*, JD SUPRA (July 19, 2019), https://www.jdsupra.com/legalnews/new-york-state-data-privacy-law-fails-39258/.

255 Nicole Lindsey, *New York Privacy Act Would Be Considerably Tougher Than California's Bill*, CPO MAG. (June 24, 2019), https://www.cpomagazine.com/data-protection/new-york-privacy-act-would-be-considerably-tougher-than-californias-bill/.

256 Ropek, *supra* note 252.

257 Lindsey, *supra* note 255.

258 Ropek, *supra* note 252.

259 Russell Brandom, *This Plan Would Regulate Facebook Without Going Through Congress*, VERGE (Apr. 12, 2019), https://www.theverge.com/2018/4/12/17229258/facebook-regulation-fiduciary-rule-data-proposal-balkin.

260 *Id.*

261 S.B. 120, 191st Reg. Sess. (Mass. 2019).

262 Mark Quist, *Comprehensive Data Privacy Legislation Introduced in Massachusetts—Includes Private Right of Action Without a Need To Prove Harm*, TECH. L. DISPATCH (Feb. 10,

other proposed state privacy regulations, the Massachusetts Act creates various rights for consumers.[263] These rights include the right to request deletion of collected personal information (the right to be forgotten); the right to request a copy of collected personal information; and the right to notice "at or before the point of collection" of the personal information that will be collected and disclosed and the purpose of such collection or disclosure.[264] It also mirrors the GDPR in that consumers may prevent businesses from disclosing their information to third parties.[265] The bill is yet to be adopted but has been hailed as one of the "tougher" laws that demands more from businesses when protecting consumer privacy.

One of the most important updates to state privacy laws is Delaware's 2017 update to its data-breach notification law.[266] Like the GDPR, Delaware's privacy law requires businesses to maintain updated, proactive security policies and procedures for its handling of personal data.[267] It also expands the definition of "personal information" to include various different types of data that the GDPR also governs, such as medical information, biometric data, and electronic signatures.[268] Additional breach notification requirements are imposed on businesses as well, which is important considering the number of technology businesses that are incorporated in the state of Delaware.[269] In terms of scope, Delaware's laws mirror the GDPR by applying to all businesses that conduct business in the state.[270] However, unlike the GDPR, yet similar to some of the other proposed state provisions, it does not provide a private right of action which limits liability for some of the larger companies that have breached data privacy standards in the past.[271]

2019), https://www.technologylawdispatch.com/2019/02/privacy-data-protection/comprehensive-data-privacy-legislation-introduced-in-massachusetts-includes-private-right-of-action-without-a-need-to-prove-harm/.

263 *Id.*

264 *Id.*

265 *Id.*

266 H.B. 180, 149th Gen. Assemb., Reg. Sess. (Del. 2017).

267 *Id.* at 1.

268 *Id.* at 3.

269 *Id.* at 4.

270 *Id.*

271 David Krone, *Delaware Amends Data Breach Notification Law To Require Reasonable Data Security and Expand the Scope of Personal Information Requiring Notice*, TECH. L. DISPATCH (Aug. 28, 2017), https://www.technologylawdispatch.com/2017/08/privacy-data-protection/delaware-amends-data-breach-notification-law-to-require-reasonable-data-security-and-expand-the-scope-of-personal-information-requiring-notice/.

V. THREE COMPARISONS OF DATA PRIVACY REGULATION

A. Comparing Regulatory Choices

1. Opt-in versus Opt-out

The CCPA was created to address not only the global shift toward privacy regulation ignited by the GDPR but also the prevention of future harm to consumers that could arise from another situation like the Cambridge Analytica scandal.[272] Though the CCPA was certainly inspired in part by the GDPR, it does not necessarily follow that compliance with one will amount to compliance with the other. The two regulations take different approaches in scope, obligations imposed on businesses, and consumer rights.[273] Some of these differences stem from the fact that the CCPA limits its application to California, whereas the GDPR is applicable in multiple countries, but also from the fact that U.S. and European values differ with respect to priorities in data-privacy regulation. For instance, the U.S. has historically protected the right to free speech, including the free speech of non-natural persons (specifically ISPs as evidenced by Section 230 of the CDA),[274] whereas Europe has often taken the approach that individual rights should be the primary consideration when crafting privacy regulations.[275]

In practice, these differences translate into the two 'different basic user consent mechanisms. While the GDPR and the CCPA both revolve around requirements that mandate that businesses get users consent on certain data collection and processing activities, consent mechanisms provided by the laws significantly differ in terms of opt-in and opt-out options.[276] Opt-in is the process that describes the positive action in which a user takes an affirmative action to offer their consent.[277] The most common way we see opt-in methods implemented is through checkboxes, where the users take action by checking the box that denotes their consent.[278] On the other hand, opt-out is the process in which a user withdraws or refuses consent for certain actions to be carried out.[279] Users with an opt-out option can uncheck a marked box or withdraw consent by changing their preferences after the original point of consent. Under the GDPR,

---

272 Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 104 MINN. L. REV. (forthcoming 2020).

273 *Id.*

274 47 U.S.C.A § 230 (West 2020).

275 Chander et al., *supra* note 272.

276 *Id.*

277 *Id.*

278 KJ Dearie, *Opt In vs Opt Out*, TERMLY (Aug. 10, 2018), termly.io/resources/articles/opt-in-vs-opt-out/.

279 Chander et al., *supra* note 272.

users' consent must be opt-in through affirmative action, instead of opt-out.[280] Although the GDPR does not specifically ban opt-out consent, the Information Commissioner's Office ("ICO") says that opt-out options "are essentially the same as pre-ticked boxes, which are banned."[281] On the other hand, the CCPA allows opt-out options in certain cases. It provides for the ability to opt out of the sale of personal information for individuals 16 years of age or older while requiring businesses to gather opt-in consent for children younger than 16 years old from either the children (if they are 13+ years old) or from their parent or guardian.

The respective scopes of the GDPR and the CCPA also differ in their application to businesses, or "data controllers and processors." The GDPR's reach is significantly broader as it applies to data subjects generally, which the law defines as "identified or identifiable natural persons."[282] Therefore, the GDPR's protection is not limited to citizens of the EU. In contrast, the CCPA protects consumers that are California residents regardless of whether they presently reside in the state or are outside of the state for a "temporary or transitory purpose."[283] It does not lend the same protection to individuals who are residing in California on a temporary basis.[284] The CCPA also does not afford protection to personal data in all circumstances as the GDPR seems to, but is instead limited to the data of consumers who are customers of household goods and services, employees, and businesses participating in business-to-business transactions.[285]

Both laws have extraterritorial effects. The CCPA protects California residents even outside of the state, while the GDPR applies to all data controllers and processors that are either established in the EU or that process data in connection with offering goods and services in the EU.[286] However, as a state-specific provision, the CCPA only applies to for-profit entities doing business in California that have a gross revenue exceeding $25 million; annually buy, receive, sell, or share, the personal data of more than 50,000 consumers; and derive 50% or more of their annual revenues from selling consumer information.[287]

---

280 *Id.*

281 INFO. COMM'R'S OFF., *Consultation: GDPR Consent Guidance* (Mar. 2, 2017), https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf.

282 GDPR, *supra* note 1, art. 4.

283 CAL. CODE REGS. tit. 18 § 17014 (2020).

284 CAL. CIV. CODE § 1798.140 (West 2020).

285 *Id.*

286 GDPR, *supra* note 1, art. 3.

287 CAL. CIV. CODE § 1798.140(c).

The GDPR and CCPA also take different approaches to specific protections regarding children. The CCPA is beholden to standards for juvenile protection that already exist within the U.S. For instance, the COPPA is not nullified by the existence of the CCPA, but rather, the CCPA adds to the existing federal protections. The CCPA prohibits the sale of personal information of any consumer under the age of 16 without consent.[288] Children between the ages of 13–16 can provide consent to data processing of their own volition, but to process data for children younger than 13, businesses must necessarily obtain the 'parents' consent.[289] The GDPR similarly restricts the ages at which children may provide consent to data processing. But instead of setting a range, it sets a default for consent at age 16 and allows Member States to tailor their provisions and to lower the age to as young as 13.[290] This also results in variable standards in the EU for this and other provisions that allow state-specific tailoring. The EU also goes a step further in requiring that children who are able to consent to data processing receive an age-appropriate privacy notice, ensuring that they understand how their data will be used.[291]

The GDPR also creates specific rights for individuals, whereas the CCPA either provides no comparable right or substantially less rights. The GDPR provides a robust right to data subjects to access their personal data, including receiving copies of their personal data and obtaining information on the data processing procedures of data controllers.[292] The CCPA only allows consumers to request disclosure of their personal information, which is limited to a written disclosure.[293] The right to be forgotten is protected under both laws, but the CCPA gives businesses much more autonomy in deciding whether to refuse the request while the GDPR provides six distinct instances in which a consumer can request deletion.[294] Both laws require that a valid request to data deletion is followed by a reasonable effort to instruct other data processors or service providers to delete the same individual's information.[295] The GDPR also secures individuals' right to rectification of incorrect or incomplete personal data or to restrict processing of personal data under certain circumstances.[296] The CCPA provides no comparable right in this regard aside from the right to opt-out in instances where one's personal information is being sold to third parties,

---

288 *Id.* §§ 1798.120(c)–(d).

289 *Id.*

290 GDPR, *supra* note 1, art. 8.

291 *Id.*

292 *Id.* art. 15.

293 CAL. CIV. CODE § 1798.100(d).

294 *Id.* § 1798.105; GDPR, *supra* note 1, art. 17.

295 CAL. CIV. CODE § 1798.105; GDPR, *supra* note 1, art. 17.

296 GDPR, *supra* note 1, art. 18.

another provision meant to protect against instances of data mishandling like that of Facebook and Cambridge 'Analytica in 2016.[297]

Private rights of action differ substantially under the two laws, the 'CCPA being the narrower of the two. Under the GDPR, an individual may bring a private right of action for any damage, material or non-material, caused by a data processor or controller that breaches the law.[298] Only certain circumstances allow for private rights of action under the CCPA.[299] Additionally, companies are given considerable flexibility under the CCPA compared to the GDPR and are allowed a 30-day period within which to cure any data violations, preempting a right of action.[300] Damages are also limited under the CCPA and range from $100 to $750 per consumer per incident.[301] In lieu of monetary damages, a U.S. court may also opt to provide injunctive relief under the CCPA.[302] Violations of either law could amount to significant financial liabilities for companies. Specifically, civil penalties can result in fines ranging from $2,500 to $7,500 under the CCPA[303] whereas administrative fines under the GDPR are capped at €20 million, or 4% of annual global revenue, whichever is highest.[304] EU Member States also have the option to impose unique penalties that are not subject to administrative fines for violations of the GDPR.[305]

2. Deletion versus Erasure

The GDPR and CCPA also present technical differences regarding data deletion. The GDPR provides users "right to erasure" which entails data subjects' right to have their personal data removed from a controller and/or processor.[306] The CCPA similarly provides California residents "right to deletion," which allows subjects to request that a business delete any personal information about the subject that the business has collected from them.[307]

The GDPR provides users right to erasure, which has been associated with the right to be forgotten.[308] Under the GDPR Article 17, data subjects have the right to request erasure of personal data under six circumstances. Once

---

297 CAL. CIV. CODE § 1798.120.

298 GDPR, *supra* note 1, art. 82.

299 CAL. CIV. CODE § 1798.150.

300 *Id.*

301 *Id.*

302 *Id.*

303 *Id.* § 1798.155.

304 GDPR, *supra* note 1, art. 83–84.

305 *Id.* art. 83.

306 *Id.* art. 17.

307 CAL. CIV. CODE § 1798.105.

308 GDPR, *supra* note 1, art. 17.

requested, data controllers must also take reasonable steps, taking into account available technology and the means available to the controller, including technical measures, to inform any other data controllers also processing the data that the data subject has requested the erasure of any links to, or copy or replication of, that personal data.[309] In practice, this means that data collectors are expected to take reasonable steps, by implementing technical measures, to inform other websites that a particular individual has requested the erasure of his or her personal data. However, this right to erasure is not an absolute right. Article 17 of the GDPR provides six cases in which the data subject may request the erasure of his or her personal data.[310]

The CCPA also provides a similar right to consumers to request deletion of their personal information. However, the request can only be made regarding data that has been collected from them directly by the California business.[311] In other words, unlike the GDPR, data deletion under the CCPA can be requested only if the data is directly collected by the business. Following Senate Bill 1121, consumers can access this right in a "form that is reasonably accessible."[312] Once data deletion is requested, the business must instruct its service providers to delete the data.

While an individual can request that his or her personal information is deleted under either law, what differentiates the two laws is the conditions under which a deletion request can be refused. The GDPR gives five such exemptions, which are all shared by the CCPA with one exception. The CCPA adds an exemption when maintaining the personal information is necessary for reasons of public health. However, in addition to the GDPR's list of exemptions, the grounds for refusal by businesses for data deletion is broader under the CCPA, as it provides nine exceptions to the right of the consumer to delete information. Namely, the CCPA includes the so-called "First Amendment exception," which provides exemption for requests if they interfere with a right to "[e]xercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law."[313]

---

309 *Id.* This is the main difference between GDPR and CCPA, and the reason why it's called the "right to be forgotten." Personal data must be deleted not only from the website of which the data subject requested the erasure, but also from other websites, links, copies, etc. ensuring total erasure from the Internet.

310 *Id.*

311 CAL. CIV. CODE § 1798.105.

312 *Id.* § 1798.130.

313 *Id.* § 1798.105(d)(4).

B. Technology Perspective: Portability Across the Atlantic

The adoption of new data protection laws has led to the introduction of new rights for data subjects. Data portability stands out among these rights.[314] The goal of portability is, on the one hand, to foster information rights and, on the other hand, to promote a level playing field in the flow of data across the internal market. Indeed, data portability would allow individuals to enjoy a broader framework of informational self-determination,[315] and would also constitute a limit to the increasing power of some business over personal data.[316]

The GDPR recognizes the right of the data subjects to receive their personal data in a structured, commonly used, and machine-readable format as well as the right to transmit that data to another controller without hindrance from the controller from which the personal data was provided. In other words, data portability would be a two step-right: first, the users should receive their personal data and, second, the data controller is required to transmit it. This right is not absolute but is instead balanced with other fundamental interests, especially those of natural persons and of the data controller. The GDPR clarifies that the right to data portability "shall not adversely affect the rights and freedoms of others."[317] Likewise, the GDPR provides another wide balancing clause to protect the exercise of the right of erasure. This is why portability is a different concept; it does not involve the erasure of data, but instead, the transmission of data. Therefore, the data subjects can enforce both rights against the data controller according to the conditions which limit the application of both data subjects' rights.

The GDPR specifies that the right to data portability applies only when the processing is carried out by automated means and is based on consent[318] or on a contractual agreement.[319] These two conditions balance other conflicting interests, especially that of the data controller, and limit portability to just two legal bases of processing. This excludes portability in cases of compliance with a legal obligation to which the controller is subject[320] and in cases of protecting

---

314 *See* Paul De Hert, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay et al., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, 34 COMPUT. L. & SEC. REV. 193 (2018).

315 *See* Gabriella Zanfir-Fortuna, *The Right to Data Portability in the Context of the EU Data Protection Reform*, 2 INT'L DATA PRIV. L. 149 (2012).

316 *See* Bart van der Sloot, *Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation*, 4 INT'L DATA PRIV. L. 307 (2014).

317 GDPR, *supra* note 1, art. 20(4).

318 *Id.* art. 9(2)(a).

319 *Id.* art. 6(1)(b).

320 *Id.* art. 6(1)(c).

the vital interests of the data subject or of another natural person.[321] Moreover, the data controller is required to transmit the data according to the data subjects' request only if technically feasible. The right to data portability does not require data controllers to implement processing systems which are technically compatible with other organizations.[322] This information should be provided free of charge.[323] Nevertheless, where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested. The controller may also refuse to act on the request. In both cases, the controller should be able to demonstrate that data subjects' requests were manifestly unfounded or excessive.

On the other side of the Atlantic, the CCPA also deals with data portability.[324] In particular, it provides a two-step scheme, similar to the GDPR. When receiving a verifiable consumer request to access personal information, businesses shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required.[325] The delivery of this information could be performed by electronic means and, in this case, the information shall also be provided "in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance."[326] If technically feasible, the technical format should enable the transmission of the information to another entity due to its readily useable format.[327] Nevertheless, the CCPA limits portability when the number of requests from the same consumers exceeds two in a 12-month period.[328]

The CCPA also specifies that the disclosure of information to the consumer shall cover the 12-month period preceding the business's receipt of the request. This information should be delivered in writing through "the consumer's account with the business . . . or by mail or electronically at the consumer's option . . . in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance."[329] Businesses shall disclose and deliver the information to consumers within 45 days of receiving a verifiable consumer request from the consumer.[330] The business shall

---

321 *Id.* art. 6(1)(d).

322 *Id.* recital 68.

323 *Id.* art. 12(5).

324 CAL. CIV. CODE § 1798.100(d) (West 2020).

325 *Id.*

326 *Id.*

327 *Id.*

328 *Id.*

329 *Id.* § 1798.130(a)(2).

330 *Id.*

promptly take steps to determine whether the request is a verifiable consumer request.[331] However, this assessment does not extend the limit of 45 days; instead, the time period to provide the required information may be extended only once by an additional 45 days when reasonably necessary, provided the consumer is provided notice of the extension within the first 45-day period.[332]

There are several similarities between the CCPA and the GDPR when it comes to the right to data portability. Both the CCPA and the GDPR allow data subjects and consumers to rely on this right to obtain access to data and to transmit it to another data controller. Nevertheless, there are also relevant differences. One of the most evident examples consists of the lack of obligation for businesses to transmit data to other business. Indeed, the CCPA would leave this transmission to consumers' responsibility, thus exempting businesses from any responsibility concerning the transmission of consumers' data. From a broader perspective, the different constitutional standpoints of the two instruments leads to two different interpretations of "portability." In the EU framework, the data subject's rights also express constitutional values enshrined in supranational charters; in the U.S. framework, this right still reflects an economic dimension linked to the relationship between businesses and consumers.

Data portability can be an opportunity to foster the role of data subjects and consumers respectively vis-à-vis data controllers and businesses. In other words, it would allow the move from a vertical and asymmetrical relationship to a horizontal standpoint where individuals can rely on new rights in the information society. Nevertheless, it is worth mentioning that the general exercise of this right is not without any consequences. The GDPR shows to be aware of the risks of an uncontrolled spread of this right for the business sector, which is why this right has been limited according to specific conditions aimed to protect data controllers and the fundamental rights of other data subjects.

C. Political Economy Perspective: Privatization or Public Enforcement?

New rules and their effectiveness are not the only concern at stake in the field of data protection. The Balkanization of data protection law is not just a matter of fragmentation of rules around the world. Even more importantly, one of the primary issues is the increasing consolidation of the role of private businesses (e.g., online platforms) in the enforcement of public policies online. The growing trend toward the recognition of private actors with functions traditionally vested in public authorities cannot be ignored. The *Google Spain v. AEPD* case has already shown how the lack of norms could not always impede public actors from recognizing new obligations for private actors (in this case, a search engine) in ensuring the public enforcement of online regulation.

---

331 *Id.*

332 *Id.*

Nonetheless, this general trend is not without consequences. In *Google Spain*, the reasoning of the court has not only entrusted a business actor with the decision over users' request of delisting, but it has also failed to take into consideration the burden that such an obligation would raise for search engines. While the e-Commerce directive exempts providers from a general obligation to monitor, the court extends its framework of liability by horizontally interpreting data protection law in light of the constitutional protection recognized by Articles 7 and 8 of the European Charter of Fundamental Rights. The ECJ has delegated to private actors (i.e., Internet search engine service providers) that carry out activities of public interest, balancing the right to information and the right to be forgotten.

Beyond the right to be forgotten, the GDPR has even extended the role of private actors by introducing a flexible notion of responsibility and risks under the notion of accountability.[333] The GDPR has opened the doors toward a comprehensive, risk-based approach, especially based on the principle of accountability of the data controller. As analyzed above, the principle of accountability requires the controller to prove compliance with the GDPR's principles by establishing safeguards and limitations based on the specific context of the processing, especially considering the risks for data subjects. This recognition leads the data controller to play a crucial role in concretely deciding how to apply the rules established by the GDPR based on an internal (and ex-ante) assessment of the risks to data subjects. This tendency towards privatization of enforcement is compelling and does not belong only to the realm of data protection but also in the framework of speech.[334] More specifically, the ability of online platforms to moderate content while maintaining their exemption of liability is a clear example of how private enforcement is spreading across sectors.[335]

This situation is not neutral from a political economy perspective. In the digital realm, as underlined by Pasquale, digital firms are no longer market participants since they "aspire to displace more government roles over time, replacing the logic of territorial sovereignty with functional sovereignty."[336] Platforms like Facebook or Google can be easily compared to entire regions of

---

333 GDPR, *supra* note 1, art. 5.

334 *See* Giovanni De Gregorio, *Democratising Online Content Moderation: A Constitutional Framework*, 36 COMPUT. L. & SEC. REV. 105374 (2020).

335 *See* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018)

336 Frank Pasquale, *From Territorial to Functional Sovereignty: The Case of Amazon*, LPE PROJECT: BLOG (Dec. 6, 2017), https://lpeproject.org/blog/from-territorial-to-functional-sovereignty-the-case-of-amazon/.

the world,[337] and have been defined as "company-town."[338] Therefore, the ability of U.S. states to deal with data protection issues is not just a matter of the complexity in regulating new technological frameworks, but also from the public dependency from the private sector for reasons of surveillance or other public purposes.[339]

Balkanization, therefore, does not involve only legal fragmentation, but also the increasing blurred lines between the public and private realms. The increasing overlaps between these two dimensions leads to wondering if there are remedies that can be proposed to face this imbalance of power in the field of data. The U.S. approach does not seem to be concerned with these risks, and the lack of federal legislation is one of the examples. Nonetheless, even if the GDPR constitutes a crucial step forward in the EU policies, it has just mitigated the increasing power of business actors in the private sector without solving the current situation of Balkanization. The GDPR still shows fallacies that would be hard to face with a lack of regulatory adjustments. It is true that the ECJ has not had many opportunities to interpret the GDPR framework to face the aforementioned situation, but relying just on judicial activism could lead to increasing the process of fragmentation, undermining legal certainty.

In *Google Spain SL v. AEPD*,[340] the ECJ interpreted the scope of application of the right to be forgotten by clarifying that EU law does not require a search engine to delist content globally. It is for a Member State to make this decision at the domestic level. This decision was based on the risks that a global extension of delisting would have led to consequences for the protection of freedom of expression from an international perspective. The right of freedom of expression does not enjoy the same degree of protection across the world. Despite restricting an individual's right, this decision would lead to a more controlled framework over private enforcement. In other words, this decision is an important step for the role of public actors in the information society. This approach would indeed foster the principle of the rule of law by providing more guidelines of the right to be forgotten online in the field. It is true that the right to delist could be limited just to EU territory, but the increase of legal certainty would lead to positive consequences for the protection of rights and freedoms on a global scale. However, this approach, which would lead to a turning point fostering the rule of law, is still at the beginning stages, but it is likely to become the standard in the information society.

---

337 *See* Anupam Chander, *Facebookistan*, 90 N.C. L. REV. 1807 (2012).

338 Tal Zarsky, *Social Justice, Social Norms and the Governance of Social Media*, 35 PACE L. REV. 154, 166 (2015).

339 *See* Niva Elkin-Koren & Eldar Haber, *Governance by Proxy: Cyber Challenges to Civil Liberties*, 82 BROOK. L. REV. 105 (2016).

340 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317, ¶ 80 (May 13, 2014).

VI. CONCLUSION

As scholars have shown, particularly through analyzing the laws in Brussels and California, the diffusion of the GDPR in terms of business compliance and circulation of regulatory ideas has influenced businesses and progressive legal practices worldwide. However, when addressing the reception of the GDPR by U.S. regulators and looking into administrative path dependencies, the political economy behind data privacy regulations, and the way in which Silicon Valley companies have spurred technological innovations, a comparison between EU and U.S. data privacy regimes shows that rather than convergence, we are likely to see Balkanization of regulations. Such fragmentation might lead to an increased workload for lawyers committed to data-privacy compliance, increasing litigation before courts through a variety of regulatory paths and reflecting the compromises made by regulators, courts, consumers, and businesses *vis à vis* the different political economic models and culture in which they are embedded.

The challenges raised by the Balkanization of data-protection laws are not just linked to legal certainty and the rule of law due to the increasing overlap between different systems across the globe. It is also a matter of decentralization of powers towards private actors operating on a global scale. This does not imply that the issue of Balkanization does not involve fragmentation and related consequences for data protection legal framework. But, focusing just on legal certainty could provide a partial picture of the asymmetries of powers which affect the political economy. Before these challenges, the phenomenon of Balkanization led legal scholars to find answers to mitigate the aforementioned situation. In different ways, the GDPR and CCPA have tried to provide answers to these challenges. They provide converging solutions to the issue of data protection in the information society, even if the two approaches are naturally characterized by a different constitutional framework and political view over the horizontal exercise of powers between private actors.

It is time to find common principles, which can harmonize data-protection law on a global scale. This process should not be guided only by important regulatory choices like extending the territorial scope of the application of the GDPR or opt-in versus opt-out mechanisms, but also a broader public policy goal to find a common framework that can provide enforceable rights to individuals or collectivities participating in a more egalitarian digital economy and democratic digital public sphere.