Europa Kolleg Hamburg
Institute for European Integration

DISCUSSION PAPER
NO.04/2020

# BRIDGING THE GAP IN TRANS-ATLANTIC DATA PROTECTION

Eric Maldonado

*As technology continues to innovate at lightning speeds and technology becomes more central to everyday life, personal data must be protected. In 2017, the passage of the General Data Protection Regulation (GDPR) in the European Union set an important precedent in the world of data protection law. Building upon the Data Protection Directive (95/46/EC), the GDPR has taken the fundamental right to privacy and extended it to the transmission of personal data. The United States of America, however, offers no such protection at the federal level – the right to privacy within the U.S. is not absolute. This article will comparatively present the pattern of case law and legislation in the EU that led to the General Data Protection Regulation, and then the pattern of case law and legislation leading to data protection law(s) in the United States of America. The contrasting degrees of protection within the two regimes is a large discrepancy; the collection and transmission of personal data is protected by law in the EU and the US differs to such a degree that companies like Facebook, have had to drastically alter their services in Europe to comply with the stringent requirements of the GDPR. The paper continues on to addresses how personal data protection is being addressed by lawmakers vis-à-vis competition law and anti-trust regulation in the EU. While it may be difficult for the United States to develop a sweeping, federal-level piece of legislation like the GDPR, the increasing success of laws protecting personal data vis-à-vis competition law points to an area in which the U.S. and the E.U. can more easily harmonize their laws and protections. Finally, the paper offers a comment on the future of the transatlantic relationship and the role data protection law could play in strengthening that relationship.*

**KEYWORDS**

Data protection, GDPR, privacy, fundamental right, competition, policy, transatlantic, USA, Europe, regulation, directive, Schrems, Safe Harbor, coordination, technology

# Content

# 1 Introduction

Technology moves quickly. In 1965, Intel co-founder Gordon E. Moore predicted that the number of components built onto silicon microchips would increase by a factor of two, every two years.[1] Dubbed "Moore's Law", this model for the general development of technology has held true for over six decades.[2] Today, computing speeds have become so fast, that in years to come that the biggest foreseeable obstacle to future improvements are the physical limits of our universe – namely, the speed of light, i.e. the speed at which electrons move through wire. In the past, collecting, analyzing, and using sets of data was slow and expensive: most, if not all of the data collection and calculations had to be done manually.[3] However, as data collection (and storage) techniques developed, using computers for data analysis became exponentially easier, and opportunities to collect, retain, and exploit such information have likewise become easier. As electronic commerce took off, businesses then had the ability to save other information, such as credit card numbers, home addresses, and social security numbers: the advent of social media added yet another dimension to the types of data and information on individuals that could be attributed to individual users.[4] As technology becomes more central to everyday life, peoples' lives, and personal data, must be protected.

The right to a privacy is one that is ostensibly both in the EU and in the United States.[5] However, In spite of the right to a private life that the EU and the US both guaranteed by law, the right to privacy of personal data is relatively new; the right to a private *digital* life continues to be an incessant effort by regulators to catch up to the pace of technological innovation and the digitization of private life. The law is struggling to catch up to the rapid rate of development and innovation related to the use of personal data. The rights of privacy for individual users must be articulated, and laws and guidelines must continue to be developed to ensure that private information remains private, and that technology's intrusive tendencies do not encroach upon the fundamental right to privacy of an individual. Today, the European Union continues to push to be a global leader in data protection, which begs the question: How might legislators in Brussels continue to innovate, while not setting restrictions that leave the US too far behind and hinder the flow of data across the Atlantic?

---

[1] See Gordon E Moore, "Cramming More Components onto Integrated Circuits," (McGraw-Hill New York, NY, USA:, 1965).

[2] M Mitchell Waldrop, "The Chips Are Down for Moore's Law," *Nature News* 530, no. 7589 (2016).

[3] Sebastian Heselhaus et al., *Handbuch Der Europäischen Grundrechte*, Second ed. (Beck, CH, 2020), 549-52.

[4] Joseph Bonneau and Sören Preibusch, "The Privacy Jungle: On the Market for Data Protection in Social Networks," in *Economics of Information Security and Privacy* (Springer, 2010), 15. "In general, far more personal data is collected than is needed for a user to interact with a social networking service, particularly gender and birth date information."

[5] Article 8, European Convention on Human Rights (ECHR); U.S. Constitution, amend. 4, (Bill of Rights).

To answer this question, Part I of this article will comparatively present the pattern of case law and legislation in the EU that led to the General Data Protection Regulation, and then the pattern of case law and legislation leading to data protection law(s) in the United States of America. The contrasting degrees of protection within the two regimes is a large discrepancy; the collection and transmission of personal data is protected by law in the EU and the US differs to such a degree that companies including, *inter alia,* Facebook and Google, have had to drastically alter their services in Europe to comply with the stringent requirements of the GDPR.[6] Part II continues on to addresses how personal data protection is being addressed by lawmakers vis-à-vis competition law and anti-trust regulation in the EU. While it may be difficult for the United States to develop a sweeping, federal-level piece of legislation like the GDPR, the increasing success of laws protecting personal data vis-à-vis competition law points to an area in which the U.S. and the E.U. can more easily harmonize their laws and protections. Finally, the paper will conclude with a short comment of what can be learned from these differences in approaches, and how they might influence future data protection policy. Strengthening the similarities and minimizing the gap in legislative protection of personal data may help to strengthen trade, political attitudes, and generally, the important transatlantic relationship between the EU and the US.

The maintenance of a strong transatlantic relationship is vital for the future. As the E.U. and the U.S. continue their diplomatic partnership and aim to strengthen their relations, it is vital that neither party becomes disenfranchised from the other, either consciously or unconsciously, through disparities in the development of law. A unified transatlantic partnership is a powerful achievement in times of turbulent geopolitics.

> *"When such nations embark on the project of creating an economic community, the unification of the legal regime concerning business transactions is bound, sooner or later, to become an issue of considerable political importance."* [7]

[6] Respectively Judgment of 3 October 2019, Case C-18/18, *Glawischnig-Piesczek v Facebook Ireland*, ECLI:EU:C:2019:821; Judgement of 6 October 2015, Case C-362/14, *Schrems,* ECLI:EU:C:2015:650; Judgement of 13 May 2014, Case C-131/12, *Google Spain,* ECLI:EU:C:2014:317.

[7] Mathias Reimann and Reinhard Zimmermann, *The Oxford Handbook of Comparative Law* (Oxford University Press, 2019), 559.

# 2 A Tale of Two Regimes

## 2.1 International Beginnings

European data protection law began its development in sync with international law. Beginning in 1948, the right to protection of personal privacy, and moreover, its recognition as a fundamental right, was first enshrined by the United Nations in Article 12 of the Universal Declaration of Human Rights.[8] Shortly thereafter, the 1950 European Convention on Human Rights (ECHR) was organized aiming to bring the countries party to the Council of Europe closer together by streamlining the human rights guaranteed to the citizens of European countries across several Member States. Article 8 ECHR ensures a guarantee of private life and became the basis of the further development of data protection law in the European Communities, and later, the European Union.

Further provisions for the privacy of personal information in International Law came in 1966, when the "unauthorized collection of storage of personal information" was articulated in the International Pact for Civil and Political Rights.[9] But, in 1980s rapid technological change introduced a new understanding of the term 'privacy'.[10] Once defined as simply the right to be left alone, privacy has now become a term to mean something more.[11] In 1990 further privacy guidelines were included as instruments in the UN Resolution for protection in the automatic processing of personal data.[12]

## 2.2 The Discovery of European Data Protection Law

Protection of electronically transmitted and collected data was first enshrined within European Law in 1995 with the passage of the Data Protection

[8] UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III).
[9] UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
[10] Heselhaus et al., *Handbuch Der Europäischen Grundrechte*, 550.
[11] Compare to Samuel D Warren and Louis D Brandeis, "Right to Privacy," *Harvard Law Review* 4 (1890).
[12] General Assembly Resolution 44/95, *Guidelines for the Regulation of Computerized Personal Data Files*, A/RES/44/95 (15 December 1990).

Directive 95/46/EC.[13] The directive clearly articulated the importance of data, its privacy, and the necessity of protecting it and its free movement within the European market.[14] The European Commission solidified the foundation of data protection in Europe began by articulating a definition for personal data and recognizing that further regulation and oversight of its usage was necessary in both the public and private sectors.[15] The Data Protection Directive became the basis for all future data protection in Europe – all later legislation was built off of this directive, and it was not until the passage of the General Data Protection Regulation that this directive was officially repealed.

Only two years after the debut of the Data Protection Directive, the EC passed Directive 97/66/EC in 1997.[16] Still relatively early on in the narrative of EU data protection law, this Directive cites the rate of development of technology and the need for updates and further elaborations in the achievement of data protection law.[17] The passage of the Data Protection Directive and a new directive two years later is significant because it indicated the awareness of the need for diligent modernization in data protection legislation to reflect technology's rapid development and the revolutionized number of personal computers found in households.[18] Moreover, the new accessibility of computers brought a new wave of personal computer owners and users, and thus also brought a wave of new users to the internet as well. Specifically, the population of individuals participating in online commerce marked a serious milestone for internet regulation. Thus, the eCommerce

[13] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 24 October 1995.

[14] Directive 95/46/EC para. 3. "[T]he free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded."

[15] Viktor Mayer-Schönberger and Yann Padova, "Regime Change: Enabling Big Data through Europe's New Data Protection Regulation," *Columbia Science & Technology Law Review* 17 (2015): 320. See Art. 3 Directive 95/46/EC.

[16] Directive 97/66/EC concerning the processing of personal data and the protection of privacy in the telecommunications sector, 15 December 1997

[17] Directive 97/66/EC para. 3.

[18] For instance, from 1995 to 2000, the number of internet users in the United States of America increased 395%, from approx. 24.5 million users to 121 million users. In the same time period, Germany's number of internet users increased 1,159%, from 1.49 million to 24.62 million users. Data taken from Max Roser, Hannah Ritchie and Esteban Ortiz-Ospina (2015) - "Internet". Published online at OurWorldInData.org. Retrieved from: 'https://ourworldindata.org/internet' [Online Resource, accessed 1 April 2020].

Directive[19]was passed, once again, to further articulate existing definitions in data protection and to introduce new challenges brought about developments in the usage of electronic devices.

In addition to legislation, the discovery of European data protection law has been furthered vis-à-vis judgements at the Court of Justice.[20] From the early aughts on and before the passage of the General Data Protection Regulation, a pattern of case law and primary and secondary law in the EU shows the trajectory the protection of personal data has taken. These cases and their respective decisions/rules are the result of almost two decades of response to the lightning-fast development of data use whose apogee was the passage of the GDPR in 2017.

The first major ruling on the guarantee of a fundamental right to privacy in the Common Market came in 2003. In *Rechnungshof,*[21] it was decided through a ruling on three combined cases, that although the right to privacy and the freedom of movement of data are indeed fundamental rights, European law does not preclude national laws from defining limits to that right for the benefit of the member state. In Austria, the Rechnungshof (national Court of Audit) controls and inspects a large number of public bodies. Part of this control and inspection function is that the bodies under its control must communicate the salaries of their employees if those salaries are above a certain level.[22] The motivation behind such a requirement is to ensure that public organizations to not abuse and/or waste public funds on, *inter alia,* exorbitant executive salaries and to ensure that public funds are used, "thriftily, economically and efficiently."[23] The questions raised in the proceedings of the case(s) later referred to the CJEU concern the legality of such a provision. The defendants in the combined cases claimed that the communication of such data

[19] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

[20] Under Article 19(3) TEU, The Courts of the European Union maintain exclusive jurisdiction on the interpretation of European Law and/or the validity of acts by its organs. In cases of gaps in the Treaties of the EU, it falls upon the Court to interpret the law and set future rules vis-à-vis judicial precedent. For additional explanation of "gap filling", see J Gutiérrez-Fons and K Lenaerts, "The Constitutional Allocation of Powers and General Principles of Eu Law'," *Common Market Law Review* 47 (2010).

[21] Judgement of 20 May 2003, Joined Cases C-465/00; C-138/01; C-139/01, *Rechnungshof,* ECLI:EU:C:2003:294.

[22] Paragraph 8, Bundesverfassungsgesetz über die Begrenzung von Bezügen öffentlicher Funktionäre, BGB1 I 1997/64; See *Rechnungshof* paragraphs 3-4.

[23] *Rechnungshof,* para. 5.

violates the protections on the movement of data as set forth in the Data Protection Directive and when read in the light of the right to a private life enshrined in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Court considered the main question of these combined cases to be whether or not European law precludes national legislation that requires State bodies to collect, transmit, and publish personal data.

The final judgement determined that European law does not preclude such national laws, such as the ones in Austria that require State bodies to collect, transmit, and publish personal data on salaries, because the laws are enacted to ensure a diligent use of public funds. In a larger scope, the ruling in these combined cases set an important precedent in data protection law that followed the legal reasoning employed in earlier CJEU decisions: that although European law ensures a great deal with regards to the fundamental freedoms, it cannot preclude national legislation that limits fundamental rights for the national benefit.[24]

In *Google Spain,*[25] and what is undoubtedly one of the most landmark decisions of both European data protection law and international data protection law, the European Court was called to rule upon an issue of legal entitlement known as the, "Right to be Forgotten".[26] In the request for a preliminary ruling, the plaintiff Mr. González requested, *inter alia,* that pages published by a newspaper in 1998 containing his name in reference to a real-estate auction be removed; and in addition to removal of the pages, Mr. González also requested that Google Spain or Google Inc. be required to remove or conceal the personal data pertaining to him and would thus no longer appear in Google search results. The Court was called upon to consider whether the function that Google performs, i.e. web searches as a search engine, can be considered the "processing of personal data" as set out in the Data Protection Directive, and/or what the scope of those rights are/is. If the questions would be answered in the affirmative, could that right be enforced within the European Union?[27] As the pivotal point thereafter, the Court needed to determine if the

[24] See e.g. Judgement of 21 June 2012, Case C-5/11, *Criminal Proceeding against Titus Alexander Jochen Donner,* ECLI:EU:C:2012:370.
[25] Judgement of 13 May 2014, Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja Congzález* (cited as *Google Spain*), ECLI:EU:C:2014:317.
[26] *Google Spain,* para. 20. "el derecho del olvido[…]"
[27] *Id.*

legitimate privacy interests at hand were enough to trump the free movement of data and data processing and the economic interests of the other parties at hand, e.g. the aforementioned newspaper and Google.[28] The Court ultimately ruled that the publishing of search results, and therefore the activity in question at Google, must be interpreted as the 'processing of data' set forth in the Data Protection Directive. Furthermore, the Court ruled that, when a data subject requests that data be removed in light of their fundamental rights to privacy (Articles 7 & 8 Charter Fundamental Rights) then those rights must overrule the interests of the general public in having access to that information, as well as any economic interests relating to the continued publication of that information.[29] Worth noting is the Court's use of the phrase "as a rule" in its decision.[30] The use of the phrase is perhaps a self-conscious acknowledgement of the fact that the judgement sets a major precedent.

In 2017, the European Union passed the General Data Protection Regulation,[31] the most progressive and comprehensive legislation on data protection in the world. "It indicates Europe increasingly considers control of massive data likely plays a critical role in attaining dominance in digital markets."[32] The passage of a Regulation on data protection is, in itself, a major gesture. The passage of a Regulation is one step short of codification into the Treaties, and is immediately directly applicable and are valid in Member States as binding law.[33] The EU's other form of 'secondary' law, the Directive, aims for a degree of workable compatibility.[34] When the European Union began its protection and regulation of personal data in earnest with the Ecommerce Directive in 2000, it chose to allow a certain degree of flexibility and variation in implementation, as Directives only set forth certain goals and policy objectives. The codification of those goals, and their enforcement, is left up to the Member States.

---

[28] *Id.*

[29] Id. para. 99, "[T]hose rights override, as a rule, not only the economic interest of the operator of the search engine, but also the interest of the general public in having access to that information upon a search relating to the data subject's name[...]".

[30] *Id.*

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter cited as GDPR), OJ L 119, 04.05.2016.

[32] Stevis-Gridneff, Matina. "E.U.'s New Digital Czar: 'Most Powerful Regulator of Big Tech on the Planet'." The New York Times. The New York Times, September 10, 2019.

[33] Article 288, Treaty on the Functioning of European Union, sent. 2-3.

[34] Peter-Christian Müller-Graff, "Ec Directives as a Means of Private Law Unification," in *Towards a European Civil Code* (Netherlands: Kluwer Law International, 2011), 149.

After the GDPR, and of the utmost importance to the transatlantic relationship is *Schrems.* In the *Schrems* judgement,[35] the case was referred to the CJEU by the High Court of Ireland, after Mr. Schrems, an Austrian citizen, made a complaint to the European Data Protection Commissioner claiming that Facebook Ireland was transmitting his personal data to the United States, and that this transmission violated his rights of data privacy because of the surveillance practices of the United States government. Facebook could be arbitrarily collected, analyzed, and stored by the U.S. government. Directive 2000/520 provides that data can only be transferred to a third-party country outside of the EU when that country also "ensures an adequate level of protection…".[36] Revelations of the surveillance practices of the U.S. government showed that data collected by Facebook could be arbitrarily accessed and saved, and was therefore not subject to protections guaranteed to European citizens. At the time, the relevant legislation between the European Union and the United States was the Safe Harbor Agreement.

Although it, *prima facie,* provided for the continuation of EU data protection principles to the transmission of data into the U.S., after the High Court of Ireland referred the case to the CJEU, the CJEU determined that the legal question at issue is whether the Safe Harbor Agreement could be compatible with Directive 95/46/EC and when read in light of Article 7 of the Charter of Fundamental Rights. The Court determined that although Facebook Ireland could guarantee the degree of privacy required by European law, the transmission of data to Facebook's U.S. operation meant that the data was no longer subject to legal protections vis-à-vis European law, and thus the transmission of data violated the terms, *inter alia,* of the Safe Harbor Agreement between the United States and the European Union.

In summary, the EU has pushed forward an incredible effort to establish themselves as the gold standard of data protection in the world. In spite of the sometimes fragmented and highly debated structure of the EU, the initiative of data protection has emerged as a powerful example of the willingness and capability of the European Union to create a truly European *demos.*[37] In this case, that same demos is the

[35] Judgement of 6 October 2015, Case C-362/14, *Schrems,* ECLI:EU:C:2015:650.
[36] Case C-362/14, *Schrems,* para. 32.
[37] See e.g. Kraus, Peter A. "The European Union's Democratic Deficit and the Search for a European Demos." Chapter. In A Union of Diversity: Language, Identity and Polity-Building in Europe, 13–36. Themes in European Governance. Cambridge: Cambridge University Press, 2008.

uniquely European GDPR – a new standard of data protection for the 21st century. At the very least, it shows Europe's active effort to lead the world in data protection.

## 2.3 The Development and Current State of American Data Protection Law

Data protection in the United States is a multi-faceted issue. It is addressed as a concern of privacy; however, it is in large part viewed as an issue of consumers' rights and consumer protection against deceptive practices.[38] Compared to the European Union, the development of data protection law in the United States has been a very different process. Rather than a stepwise progress of recognition and implementation, through both legislation and reinforced by court judgement that characterized the discovery of European data protection, American data protection law has had a very sporadic process of development.

To begin, one can turn to the legislation that makes up both privacy and consumer protection in the United States. In the United States, there is no explicit or fundamental right to privacy.[39] Instead, privacy is a right pulled from Supreme Court decisions and the Bill of Rights.[40] The Fourth Amendment of the Bill of Rights was was originally established as a protection against arbitrary search and seizure,[41] but was expanded through court decision to mean the right to a private life and personal sphere in such areas as medical information, [42] membership in political organizations,[43] and a general right to anonymity.[44] The important caveat to all of these decisions and rights is that privacy is always subject to limitations, especially when read in light of the Fourth Amendment;[45] the spectre of a possible exception

[38] Federal Trade Commission Act 1914, 15 U.S.C. § 45.
[39] David Banisar and Simon Davies, "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments," *J. Marshall J. Computer & Info. L.* 18 (1999): 108-09.
[40] *Id.*
[41] Amendment IV, Bill of Rights, Constitution of the United States of America 1791, [*T]he right of the people to be secure in their persons, houses, papers, and effects, against* ***unreasonable*** *searches and seizures, shall not be violated, and no Warrants shall issue,* ***but upon probable cause****[…]* (emphasis added).
[42] *Griswold v. Connecticut*, 381 U.S. 479 (1965).
[43] *NAACP v. Alabama*, 357 U.S. 449 (1958).
[44] *McIntire v. Ohio Elections Comm.,* 514 U.S. 334 (1995).
[45] See Fourth Amendment text, note 46.

to any degree of privacy in the US is omnipresent.[46] For example, in *Smith v Maryland,* the highest court in the US, the Supreme Court of the United States (hereinafter as SCOTUS) ruled that public telephones are not subject to a "reasonable expectation of privacy" and therefore do not require a warrant to be accessed by the surveillance devices of authorities.[47]

In one of the one of the most recent rulings on data protection, the Supreme Court of the United States (hereinafter as SCOTUS) produced a judgement in *Carpenter v United States*,[48] in which it established a significant precedent for guarantees of privacy. The case revolved around an individual arrested and convicted for the armed robbery of several electronics stores. In the conviction, the petitioner relied on location and time data recorded by a wireless communications provider. Wireless communications carriers provide their services through broadcasting locations referred to as cell sites. These locations record the presence and movements of cellular devices even when a customer is not actively using the device. A record is generated at a cell site almost every minute, in a time-stamped data point named a cellular service location information (CSLI). The purpose of this type of tracking is to provide the carrier with information for, *inter alia,* roaming charges and to determine if there are areas of weak signal strength within the wireless network. The legal issue debated in the case revolved around an individual that was arrested and convicted for a series of armed robberies, a Mr. Carpenter.

His conviction was based upon evidence collection by his wireless provider. Using the time stamps and locations recorded by the CSLIs, the prosecution in the case was able to place Mr. Carpenter at the scene of the crimes committed. Upon conviction, he was sentenced to over 100 years in prison: a decision that was immediately appealed. The grounds for appeal were that the CSLIs provided by the wireless carrier were obtained and used without a warrant – a direct violation of the Fourth Amendment's constitutional guarantee of privacy vis-à-vis a protection against unwarranted search and seizure. However, upon appeal, the District Court denied the motion to suppress the cell site information, which the Court of Appeals for the Sixth Circuit upheld. Later, when brought before the SCOTUS, it was reversed and

[46] *Katz v. United States*, 389 U.S. 347 (1967).
[47] *Smith v. Maryland*, 442 U.S. 735 (1979).
[48] *Carpenter v. United States,* No. 16-402, 585 U.S.__ (2018).

remanded the decision back to the Circuit Court of Appeals on the grounds that the information provided by CSLI and furthermore relied upon to convict Mr. Carpenter was obtained without warrant and indeed violated the Fourth Amendment. As Chief Justice Roberts wrote when delivering the opinion of the Court:

> *"Here the progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers [...] drafted the Fourth Amendment to prevent."*[49]

The most significant rights to privacy in the United States exist in specific laws meant to protect the processing of personal data in specific sectors, such as medical records and financial information.[50] Moreover, because these specific protections often involve economic activities, they then fall within the jurisdiction of the Federal Trade Commission to be upheld and monitored, but not enforced.[51] Instead The Federal Trade Commission (FTC) is the highest authoritative body concerned with American consumer protection and is likewise tasked with regulating data protection in the US. Founded in 1914 through the passage of the Federal Trade Commission Act,[52] its purpose is to promote a heathy market within the US and to combat deceptive practices in the marketplace. Therefore, it can only enforce issues of data protection when they are an issue of deceptive trade practices.[53] Current consumer data protection can be generally grouped within two prevalent models, the "notice-and-choice" model, and the "harm-based" model.

In the notice-and-choice model, the belief is that businesses should work to inform consumers about what data is taken and how it is used, so that they would be able to make informed decisions on the release of their data. The harm-based model protects against specific harms which include but are not limited to physical security, security of property, economic security, and invasions into the daily lives of consumers.[54] One of the first actions taken by the FTC to protect the data of

[49] *Id.* para. 22.
[50] Fair Credit Reporting Act (FCRA) 1970, 15 U.S.C. § 1681; Health Insurance Portability and Accountability Act (HIPAA) 1996.
[51] Banisar, *supra* note 41. 109.
[52] 15 U.S.C. §§ 41-58.
[53] Banisar, *supra* note 41. 109.
[54] See 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center, at 301; 1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology, at 36-38; 1st Roundtable, Remarks of Susan Grant, Consumer Federation of America, at 38-39.; Available at

American consumers was the Fair Credit Reporting Act 1971 (FCRA). Aimed at consumer credit reporting agencies that kept records of consumer spending, financial, and other personal information, the FCRA required that agencies meet a standard of accurate, fair, and private record keeping when handling consumer data. In 2003, the U.S. Congress amended the FCRA with the Fair and Accurate Credit Transactions Act (FACT Act), that reflected the modernization of issues like identity theft.

Another major piece of legislation in American data protection history is the 1986 Electronic Communications Privacy Act of 1986 (hereinafter as ECPA).[55] The ECPA protects the privacy of the collection and storage of electronic communications and other identifying data related to individual users, like emails and user profiles being stored on servers. Similar to the original Data Protection Directive, this law was an official recognition of the need for regulation in the growing frontier of the internet. However, unlike the European Union, updates to the ECPA only came through the court decisions, and not at the federal level as new law.[56]

In summary, the state of American data protection law is fragmented at best. No single, central guarantee of data exists. Instead, apart from settled case law, Americans must rely on a patchwork quilt of laws that safeguard only certain aspects of personal data, and that only offer the fundamental of privacy with limitation. This state of the art creates serious opportunities for exploitation. With capabilities of real time data collection and electronic tracking troves of personal information be assembled that can be paired with recordings of physical movements, allowing capable individuals to gain access to personal information and patterns once impossible to track.[57] It is no exaggeration to say that data protection has developed into a completely different beast in the United States compared to Europe.

---

FTC, Exploring Privacy– A Roundtable Series, http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

[55] Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. 121 §§ 2701-2712.

[56] For example, *Crispin v Christian Audigier* 717 F. Supp. 2d 965 (2010), in which the SCOTUS ruled that communications over Facebook Messenger are protected by the ECPA.

[57] Thompson, S., Warzel, C. (2019, December 20). How to Track President Trump. Retrieved September 01, 2020, from https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html

# 3 In Comparison

## 3.1 A Comparative Look

The first striking difference between the EU and American data protection regimes is that within the EU, there is a recognized fundamental right to privacy, whereas in the United States, no fundamental right to privacy exists. The European Union's recognition of the ECHR is key in creating a legal framework basis that can foster effective data protection law. It is upon this basis that the significant pieces of European Law, i.e. the Data Protection Directive and the GDPR, have been built. Before the adoption of Europe's own Charter of Fundamental Rights, Article 8 ECHR served as the right that European data subjects could rely upon in legal proceedings.[58] Then, after the adoption of the European Charter of Fundamental Rights with the Lisbon Treaty,[59] European citizens had actionable European Law that could be relied upon as a guarantee of privacy; that right was the starting point for the GDPR.[60] What is important is that the EU related and extended the fundamental right of privacy into the electronic world of data and data processing early on and built a legal culture of laws and institutional due process surrounding data protection that continues to treat data protection and privacy a fundamental right. In the United States, no such guarantee of privacy exists, and has resulted in a different culture. Instead, privacy has been an inferred right built up from the Amendments to the US Constitution – notably the Fourth Amendment of the Bill of Rights. The reliance upon case law and the Bill of Rights alone does not offer a fundamental guarantee of privacy; the right to privacy in the US is always subject to exception.[61]

---

[58] "Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treat on European Union, include [...] promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms." Dir. 95/46/EC, preamble, para. 1.

[59] After the passage of the Lisbon Treaty in 2009, the Charter of the Fundamental Rights of the European Union (the Charter) became legally binding to all Member States.

[60] "The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the Charter)[...] provide that everyone has the right to the protection of personal data concerning him or her." Regulation 2016/679/EU, preamble, para. 1.

[61] Bill of Rights, Constitution of the United States of America 1791. See emphasis, note 43.

The second striking difference between the European and American Regimes is the fact that the EU has a major, consolidated, law outlining the framework of data protection, while the United States does not – instead the U.S. has a smattering of laws and acts that offer specific protections on certain types of financial and medical data. The GDPR is legally binding upon all Union institutions and in all Member States.[62] What's more, as a Regulation, instances arising from the process of drafting a directive into national law will not arise;[63] the text of the Regulation is, for all intents and purposes, as good as drafting a law into the Treaties. [64] Prior to the Lisbon Treaty, there existed a 'hierarchy of norms' within the European Communities; in their passage and application, Directives were viewed as 'weaker' acts than Regulations.[65] Finally, a major difference within the US there is no direct way to easily begin proceedings, claiming infringements of data protection law. In the EU, the GDPR provides for a Controller and Processor who, in addition to supervisory authorities, may be contacted in instances of security breaches.[66] The regulatory body responsible for data protection laws in the US is the FTC – a federal body that was established as a means of combating deceptive practices and defending consumer rights, often in the field of competition. Therefore, not only are the protections in the of data privacy in the US wanting, they are seldom thoroughly handled.[67]

Academic perspectives on the two regime relations are varied. One suggests that the American system is that sovereignty can and should be maintained between the individual states, but done with an awareness of federal compatibility.[68] Since data is used so often in the commercial sector, individual states could foreseeably hold this power away from the government by resisting reform at the federal level. The conflict of sovereignty and competencies against a federal centralization of power is

[62] Article 288 TFEU, Regulations are classified as primary EU law and have equal standing as articles within the Treaties.
[63] Mayer-Schönberger, *supra* note 15.
[64] Although it was not formalized within the Treaties, there was an understood differentiation between primary norms and secondary norms, in terms of the strength pursuant to a goal or topic. Paul Craig and Gráinne De Búrca, *Eu Law: Text, Cases, and Materials*, Sixth ed. (Oxford University Press, USA, 2015), 110.
[65] Trevor C. Hartley, *European Union Law in a Global Context: Text, Cases and Materials* (Cambridge University Press, 2004), 45.
[66] Articles 24 –34 Regulation 2016/679/EU (GDPR).
[67] Banisar, *supra* note 41, 109.
[68] Andrew Keane Woods, "Litigating Data Sovereignty," *Yale Law Journal* 128 (2018): 359-371.

relevant in the US as it is in the European Union: especially when it comes to cross-border internet transmission. This cross-border element, whether across national borders in European Member States, or across State borders in the US might suggest that the digital era is either beyond or eroding a border-based regulation level.[69]

In other words, as we look to the future, instead of resistance to federal centralization of data protection law, research suggests States could instead spend their time and resources developing inter-State protections that would potentially allow a degree of compatibility to each other.[70] Moreover, just as the fragmented degrees of data protection might introduce problems within the US, this fragmentation could also create problems for US companies doing international business; especially those doing business in the EU.[71]

External relations of the European Union are an important source of influence on the development and discovery of European jurisprudence through the Court of Justice.[72] The United States of America and the decisions of its Supreme Court are a significant partner in politics, trade, and global economic influence, and therefore will continue to have an influence on the evolution of European law. Because the two the status of Data Protection Law across the Atlantic differs to such a significant degree, a focus on the harmonization of DPL is thus needed from researchers and legislators alike. As the next section indicates, there ample room to do so within the field of competition law.

## 3.2 Competition Law and Data Protection

In the United States, this culture has yet to be fully developed in spite of the body of research that has been done and is still being done in the subject area.[73] The result

[69] *Id*. 358-359.
[70] *McKay Cunningham, "Complying with International Data Protection Law," University of Cincinnati Law Review 84 (2016).* 449-50.
[71] *Id.*
[72] Koen Lenaerts and Kathleen Gutman, "The Comparative Law Method and the European Court of Justice: Echoes across the Atlantic," *The American Journal of Comparative Law* 64, no. 4 (2016): 845-46.
[73] *See inter alia*: Paul M Schwartz, "Legal Access to the Global Cloud," *Columbia Law Review* 118, no. 6 (2018).; Kenneth Olmstead and Aaron Smith, "Americans and Cybersecurity," *Pew Research Center* 26 (2017). George W Coombe Jr and Susan L Kirk, "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations," *Bus. Law.* 39 (1983).

has been a body of data protection law that can be described as sparse.[74] Instead, the United States has built a culture that intensely combats anti-competitive behavior. The US passed their first piece of legislation against cartels over 100 years ago.[75] Although the attitudes of the US and the EU may differ on the absolute guarantee of data protection rights, they have both demonstrated in their intense development of antitrust law, that keeping healthy economies is a priority. The EU places enormous responsibility into its competition authority. The proactive prevention of abusive market practices and the formation of monopolies has been repeatedly mentioned by the EU as a path of further development.

The United States has also taken a firm stand on anti-competitive behavior in the last few decades with the intent of preserving markets that foster competition and thus innovation. If the US and EU are looking to find common ground through data protection law, perhaps an enhanced focus on the harmonization of antitrust law should be pursued. This may prove the path of least resistance between two governments that have radically different views on the degree to which privacy can be legally guaranteed.

In Europe, data harvesting must now also be considered part of anti-trust regulatory analysis. The European Union's charge to set a high standard of data protection did not stop with the declaration of standards. Data security and electronic commerce are almost inseparable; the action of providing personal data to an online retailer as a modern consumer is pervasive. On the other side of those transactions, online retailers and modern companies are caught in an incessant storm of sensitive (and non-sensitive) data as the engage in their day-to-day operations. As previously mentioned, in the 1990s the use of customers' data was extremely cost-intensive. Methods of collection data were slow as they depended on the manual recording and formatting of the data. These methods were also limited in their scale(s) of application: they often only provided a snapshot of the existing parameters and information of the consumer. Furthermore, they were prone to expire. Data sets of consumers were not easily updated – updates of that data would thus mean

[74] Cunningham, "Complying with International Data Protection Law."
[75] Clayton Anti-Trust Act 1914, 15 U.S.C. §§ 12–27, § 29, §§ 52–53.

recollecting the data and then comparing the respective sets. Above all, each step required money, and would thus prove to be an expensive of a task as it was arduous.

In the modern marketplace, the use of metadata is becoming more and more popular. Metadata refers to the analysis of "data about data." The ease and speed with which individual points of data can be collected, stored, and used in calculations is almost insignificant. So much so that businesses now use amounts of data that would be nigh impossible for humans to process in a useful amount of time or manner. Furthermore, large and dominant firms have significant resources that allow them to use and analyze data without the same barriers as smaller firms. Therefore, there is a correlation between the size and value of a firm and the amount of personal data it will likely use and store. This is one of the many reasons that can explain the overlap of data protection law into the enforcement of Competition and Anti-Trust law.

The European Union has already presented examples of how data protection often serves at the as the basis for anticompetitive action by the European Union and its bodies and in the Member States as well. In both the *Facebook/WhatsApp*[76] and *Microsoft/LinkedIn* cases, the anticompetitive action taken by the European Union both had questions at their cores pertaining to the use of personal and sensitive customer data. In *Facebook/WhatsApp,* the Commission served Facebook several punitive fines for (1) providing inaccurate and deceptive information about their acquisition of WhatsApp, as well as (2) not disclosing the collection and use of personal data of WhatsApp customers.[77]

On the Member State level, Germany's Bundeskartellamt decided in a landmark decision that firms in dominant positions effectively create a monopoly when forcing users to accept their "Terms & Conditions". The decision was grounded in the fact that networks like Facebook, Twitter, Snapchat, and Instagram, occupy markets that are so specialized, that each one creates almost impassible barriers to entry in their respective markets. It follows that by occupying such a dominant position, they force user to accept terms and conditions they might otherwise oppose; not accepting the terms and conditions precludes the use of the social network and platform.[78] It is

[76] Bundeskartellamt, Case decision of 6 February 2019, ref. B6-22/16, (*Facebook*).
[77] *Id.* paras. 1-2.
[78] *Id.*

clear that the attitudes of the US and the EU are similar in stance, but could it be that the difficulties in the harmonization of the level of guaranteed data protection stem from different sources? "U.S. law and the courts are more conservative on antitrust," Mr. Kimmelman said. He added: "We've had very little, almost no enforcement against the tech sector. Europe is in the leadership role."

## 4 Conclusion: Challenges for the Future

A challenge of Big Data to consumers, programmers, and lawmakers alike is its complexity. The complexity of processes performed using large sets of data, and the complexities of their effects on individuals. Because many of these notions are exceedingly complex in their application, a criticism of data protection law has been its "linear" approach. One model of big data issues is the "wicker" model.[79] Rather than thinking of Big Data as a simple object, computer scientists and social scientists have been developing models for "systems thinking" that develop models well-suited to the complex nature of Big Data and its unique features and challenges.

Although data protection may largely apply to private entities, it can and must be applied to a largely private sphere; European data protection law now focuses on the handling and processing of personal data from a largely commercial and federal perspective at the same time. Data protection within the European Union aims to guarantee individuals the right to privacy protection from commercial agents and governments. An answer to this problem may lie in the creative new approach of tech regulators. European Data Protection law has now entered the Antitrust sphere, where European-level watchdogs are ready and willing to take action when companies like Facebook use their dominant position in the marketplace to collect and transfer customers' personal data at their own discretion.[80]

An issue that deserves attention is the economic effects of data use and data regulation. Indeed, many, if not most of the arguments made against increased data regulation assert that the efficiencies spurred by the collection of personal data help

[79] Henry Pearce, "Systems Thinking, Big Data, and Data Protection Law," *Eur. JL Reform* 18 (2016): 482.
[80] Bundeskartellamt, Case decision of 6 February 2019, ref. B6-22/16, (*Facebook*).

build economies. Additionally, some claim that the economic effects of data regulation could stifle innovation and reduce public welfare.

A conclusion to this issue may be that the governments of the US and the EU have different attitudes towards data protection. While the guarantee of a right of privacy is common between the two, the EU's government has taken a stance that far outperforms the United States and leads the world in its degree of completeness. The US on the other hand, has coupled developments in data protection with legislation that allows for surveillance and monitoring of sensitive data as a means of combating terrorism and ensuring the domestic safety of its citizens. If the two cannot find a way to explicitly compromise these points, then perhaps the key to true harmonization lies in something both entities actively and insatiably pursue: a healthy economy.

The United States was founded upon democratic ideals that included, *inter alia,* the right to pursue commerce across state borders. Similarly, the EU was founded upon the development of a free trade area and has continued to build its corpus of case law supporting the protection of a free trade area, and even a single currency area. Given the amount of experience, resources, and the priority of healthy economy in both entities, if so, much common ground already exists and attitudes towards competition law overlap, then the recommendation of this work is that the further development of data protection law must be pursued vis-à-vis the development, enhanced cooperation, and harmonization of competition law.

Put plainly if the US and the EU plan to continue strengthening their relationship through enhanced cooperation, then harmonization at the level of data protection law must take place. This proves to be a very difficult challenge when considering the social dimension of these changes. It has been made explicitly clear, both through the CJEU and through European Authorities, that the absolute guarantee of data protection rights with few exceptions is a priority of the European Union. Finally, because of the strong correlation of data usage/exchange amongst firms in dominant market positions, the continued deregulation of commerce could result in significant damages to social welfare vis-à-vis monopolistic economy deadweight losses and stagnant innovation vis-à-vis decreased competition.

# 5 Bibliography

Banisar, David, and Simon Davies. "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments." *J. Marshall J. Computer & Info. L.* 18 (1999): 1.

Bonneau, Joseph, and Sören Preibusch. "The Privacy Jungle: On the Market for Data Protection in Social Networks." In *Economics of Information Security and Privacy*, 121-67: Springer, 2010.

Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy Regulation and Market Structure." *Journal of Economics & Management Strategy* 24, no. 1 (2015): 47-73.

Coombe Jr, George W, and Susan L Kirk. "Privacy, Data Protection, and Transborder Data Flow: A Corporate Response to International Expectations." *Bus. Law.* 39 (1983): 33.

Craig, Paul, and Gráinne De Búrca. *Eu Law: Text, Cases, and Materials.* Sixth ed.: Oxford University Press, USA, 2015.

Cunningham, McKay. "Complying with International Data Protection Law." *University of Cincinnati Law Review* 84 (2016): 421.

Gutiérrez-Fons, J, and K Lenaerts. "The Constitutional Allocation of Powers and General Principles of Eu Law'." *Common Market Law Review* 47 (2010): 1629.

Hartley, Trevor C. *European Union Law in a Global Context: Text, Cases and Materials.* Cambridge University Press, 2004.

Heselhaus, Sebastian, Carsten Nowak, Manfred Baldus, Marten Breuer, Thomas Bruha, Marc Bungenberg, Wolfram Cremer*, et al. Handbuch Der Europäischen Grundrechte.* Second ed.: Beck, CH, 2020.

Lenaerts, Koen, and Kathleen Gutman. "The Comparative Law Method and the European Court of Justice: Echoes across the Atlantic." *The American Journal of Comparative Law* 64, no. 4 (2016): 841-64.

Mayer-Schönberger, Viktor, and Yann Padova. "Regime Change: Enabling Big Data through Europe's New Data Protection Regulation." *Columbia Science & Technology Law Review* 17 (2015): 315.

Moore, Gordon E. "Cramming More Components onto Integrated Circuits." McGraw-Hill New York, NY, USA:, 1965.

Moravscik, A. "What Can We Learn from the Collapse of the European Constitutional Project: A Response to Eight Critics." *Notre Europe* (2006): 1-15.

Müller-Graff, Peter-Christian. "Ec Directives as a Means of Private Law Unification." In *Towards a European Civil Code*. Netherlands: Kluwer Law International, 2011.

Olmstead, Kenneth, and Aaron Smith. "Americans and Cybersecurity." *Pew Research Center* 26 (2017).

Pearce, Henry. "Systems Thinking, Big Data, and Data Protection Law." *Eur. JL Reform* 18 (2016): 478.

Reimann, Mathias, and Reinhard Zimmermann. *The Oxford Handbook of Comparative Law.* Oxford University Press, 2019.

Schwartz, Paul M. "Legal Access to the Global Cloud." *Columbia Law Review* 118, no. 6 (2018): 1681-762.

Waldrop, M Mitchell. "The Chips Are Down for Moore's Law." *Nature News* 530, no. 7589 (2016): 144.

Warren, Samuel D, and Louis D Brandeis. "Right to Privacy." *Harvard Law Review* 4 (1890): 193.

## About the Author

**Eric Maldonado** was a visiting fellow at the Europa-Kolleg Hamburg within the "Europe and Beyond" Fellowship Program which is part of the cooperation between Europa-Kolleg Hamburg and Bundeskanzler-Helmut-Schmidt Foundation and financed through funding by the Free and Hanseatic City of Hamburg. Eric Maldonado is a doctoral candidate in European Law at Universität Hamburg. Prior to his doctoral research, he earned the Master of European and European Legal Studies (MEELS) from Universität Hamburg. He completed studies in both Business Administration and Music History at the State University of New York College at Geneseo.

**Contact:** Eric.maldo38@gmail.com

## Europa-Kolleg Hamburg
## Institute for European Integration

The Europa-Kolleg Hamburg is a private law foundation. The foundation has the objective of furthering research and academic teachings in the area of European integration and international cooperation.

The Institute for European Integration, an academic institution at the University of Hamburg, constitutes the organisational framework for the academic activities of the Europa-Kolleg.

The Discussion Papers are designed to make results of research activities pursued at the Institute for European Integration accessible for the public. The views expressed in these papers are those of the authors only and do not necessarily reflect positions shared by the Institute for European Integration. Please address any comments that you may want to make directly to the author.

**Editors**
Europa-Kolleg Hamburg
Institute for European Integration
Prof. Dr. Jörg Philipp Terhechte, Managing Director
Dr. Andreas Grimmel, Research Director
Windmühlenweg 27
22607 Hamburg, Germany
**http://www.europa-kolleg-hamburg.de**

**Please quote as follows**
Europa-Kolleg Hamburg, Institute for European Integration,
No.04/2020, http://www.europa-kolleg-hamburg.de

Europa Kolleg Hamburg
Institute for European Integration

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG