doi:10.1017/aju.2019.83

SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

THE LIMITATIONS OF EUROPEAN DATA PROTECTION AS A MODEL FOR GLOBAL PRIVACY REGULATION

*Shannon Togawa Mercer**

The consensus view is that European-style data protection (including the General Data Protection Regulation (2016/679) (GDPR)) is becoming the global standard.[1] But this view is not shared by all, with scholars pointing to divergence between European and American approaches to privacy.[2] Determining the relative influence of each model is important. Regulation of the private sector use of personal data can shape economic and social conditions, from the cost of running a business to the relationships between consumers, companies, and their governments. This essay argues that it is too soon to conclude that the European Union has won the competition to influence global data protection and privacy laws, especially as the United States finds itself in the midst of shaping and defining its own privacy regime. I will explore the GDPR's viability as a global regulatory model, raising reasons to doubt that it will ultimately dominate the privacy regulation market. First, the mere fact that the United States is likely to develop a federal privacy regime that will depart from the European model will be influential in its own right. Second, there are compelling economic reasons for private and public entities to lobby against European-style regulation.

The GDPR

The GDPR came into force on May 25, 2018 (adopted in the remaining European Economic Area (EEA) countries in July 2018)[3]—replacing the Data Protection Directive (95/46/EC) (Directive).[4] The GDPR applies extraterritorially to institutions that either have an EEA presence or target EEA individuals.[5] It regulates the

* *Attorney, Skadden.* *Thanks to Danielle Keats Citron, Gráinne de Burca, Quinta Jurecic, Julie Rheinstrom, Alan Rozenshtein, Eve-Christie Vermynck, and Tom Williams for comments on earlier drafts.*

[1] *See, e.g.*, Paul M. Schwartz, *Global Data Privacy: The E.U. Way*, 94 N.Y.U. L. Rev. 771 (2019); Mark Scott & Lauren Cerulus, *Europe's New Data Protection Rules Export Privacy Standards Worldwide*, Politico (Jan. 31, 2018).

[2] *See, e.g.*, Anupam Chander et al., *Catalyzing Privacy Law* (U. Colorado Law Legal Studies Research Paper No. 19-25, 2019); *see generally* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 Yale L.J. 1151 (2004); Greg St. Martin, *We Know You're Not Reading All Those G.D.P.R.-Related Privacy Policy Emails. Maybe You Should.*, News@Northeastern (May 22, 2018).

[3] *The History of the General Data Protection Regulation*, Eur. Data Prot. Supervisor; *see also* General Data Protection Regulation Incorporated into the EEA Agreement, Eur. Free Trade Ass'n.

[4] *See generally* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. Article 3 (L 119) 1 [hereinafter GDPR].

processing—including collection, recording, and storage—of EEA personal data, including transfers of personal data outside of the EEA. While the GDPR shares the Directive's underlying principles (including lawfulness of processing, purpose limitation, accuracy, and storage limitation), the GDPR introduces new elements to the regulatory landscape, including a maximum administrative fine up to the higher of 4 percent of global annual turnover and EUR 20 million; the possibility of collective actions (or class actions); obligations on data processors; uniform requirements concerning data breach notifications; and data subject rights, such as the right to be forgotten and data portability.

Currently, the GDPR is the most developed data protection law in the world, but questions remain about its efficacy. There have been only a few notable enforcement actions. On January 21, 2019, the French Data Protection Authority fined Google EUR 50 million.[6] In July 2019, the UK Information Commissioner's Office published two intentions to fine for GDPR violations: just under £200 million against British Airways for compromizing the personal data of five hundred thousand customers, and another against Marriott International for just under £100 million for exposing the data of nearly 340 million of its customers.[7] Regardless, the GDPR has already conditioned the global conversation about data protection and privacy regulation.

Due to its outsized market power and global influence, the EU currently enjoys a reputation as the de facto world privacy regulator.[8] As of 2018, around seventy-five non-European countries have enacted EU-style laws, and over ten of these have adopted new GDPR principles.[9] New privacy regimes in Brazil and Thailand (and new bills in India and other jurisdictions) are evidence of continued influence. Different theories exist about why EU privacy ideas have diffused this way.[10] Even the United States is not immune to the EU approach: the impending California Consumer Protection Act (CCPA) has been called a "GDPR-lite"; Washington state recently voted on (but failed to enact) an EU-style consumer data privacy bill; and the Obama administration published a Consumer Privacy Bill of Rights that leaned toward certain EU principles.[11]

But this is not the full picture. Another camp contends that declaring GDPR's victory is premature, especially in the United States. A privacy law with a distinct U.S. flavor may achieve superior market penetration. Anupam Chander, Margot Kaminski, and William McGeveran argue that the CCPA is more than just a copy and paste version of the GDPR. On January 1, 2020, the CCPA will be the most comprehensive state privacy legislation in the United States. As such, it may set "a new national equilibrium for data privacy," dictating the terms of "the march of a new American data privacy spreading to other jurisdictions."[12]

This is a catalyzing moment for the United States. The proliferation of state privacy laws will create a fractured system if there is no federal framework preempting them; recent privacy events, such as the Cambridge Analytica scandal and the Equifax breach, have raised collective public awareness; and the GDPR, not least because of its extraterritoriality, creates a standard to which the U.S. government is expected to respond. These conditions make

[6] *See CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against Google LLC* (Jan. 21, 2019).

[7] UK Information Commissioner's Office, Press Release, Intention to Fine British Airways £183.39m Under GDPR for Data Breach (July 8, 2019); *see also* UK Information Commissioner's Office, Statement, Intention to Fine Marriott International, Inc More than £99 Million Under GDPR for Data Breach (July 9, 2019).

[8] Schwartz, *supra* note 1, at 4, 30.

[9] *Id.* at 6.

[10] *Id.* at 1.

[11] *See generally* The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012).

[12] Chander et al., *supra* note 2, at 54.

https://doi.org/10.1017/aju.2019.83 Published online by Cambridge University Press

it more likely that the United States will put forward some federal privacy framework.[13] So why are the results of this constitutional moment unlikely to look like the GDPR?

Privacy Rights

Much has been written about the different baseline assumptions about privacy held in the United States and the EU.[14] The EU framework recognizes a fundamental human right to privacy,[15] whereas in the United States—where rights to certain types of privacy (from government intrusion and in sector-specific circumstances) have been legislated and adjudicated—there is no explicit constitutional right to privacy.[16] The U.S. approach to regulation is also different: instead of specific privacy regulators like the European Data Protection Board, general consumer protection bodies oversee privacy in the United States.[17] This legal patchwork leaves gaps. Lindsey Barrett explains, "If no sector-specific law applies . . . the data collector is free to collect and use what it will, subject to the Federal Trade Commission . . . unfairness and deception enforcement authority" and, as Danielle Citron explains, the authority of state Attorneys General as well.[18]

A basic application of Wesley Hohfeld's jural relations illustrates the depth of the divergence between U.S. and EU approaches.[19] Where there is no blanket data protection law and no explicit constitutional right to privacy, a company will have the liberty to use personal data and an individual will have no claim against it—a Hohfeldian liberty-right. The U.S. system sees privacy as a function of a company's liberty-right. European-style privacy law starts from the assumption that the individual has the right to control the use of her personal data as a Hohfeldian claim-right. In other words, an individual has the right to dictate how her personal data is used and other parties have duties to not violate that right. These fundamentally opposed perspectives make it unlikely that the claim-right model will carry the day in the United States.

Several alternative U.S. models have been proposed in the academic and political spheres. Neil Richards and Woodrow Hartzog argue that a framework of U.S. federal privacy governance could, and should, go beyond the CCPA and the GDPR, incorporating "societal and group-based concerns as well as civil rights-based protections," focused on "power asymmetries, corporate structures and a broader vision of human well-being."[20]

Chander, Kaminski, and McGeveran take a different approach. They argue that the CCPA, rather than the GDPR, will be the basis for U.S. state and federal laws.[21] Surface-level similarities exist: the CCPA, like the GDPR, builds off of Fair Information Practice Principles—historically foundational principles for

[13] For a critical analysis of the federal and state privacy law systems in the United States, see generally Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 Lewis & Clark L. Rev. 595 (2016).

[14] *See, e.g.*, Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L.J. 115, 120 (2017).

[15] Chander et al., *supra* note 2, at 12.

[16] *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965). *See generally* Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890); William Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960); and the California Law Review Symposium on *Prosser's Privacy at 50*, Vol. 98, No. 6 (Dec. 2010).

[17] Chander et al., *supra* note 2, at 13.

[18] *See* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR and Information Fiduciaries*, 42 Seattle U. L. Rev. 1057, 1059 (2019); *see also* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 Notre Dame L. Rev. 747 (2016); Schwartz & Peifer, *supra* note 14, at 120; Anu Bradford, *The Brussels Effect*, 107 Northwestern U. L. Rev. (2012), *supra* note 12, at 22–23.

[19] *See generally* Wesley Newcomb Hohfeld, *Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays*, 26 Yale L.J. 710 (1917).

[20] Neil M. Richards & Woodrow Hartzog, *Privacy's Constitutional Moment* 61 B.C. L. Rev. [2], [54] (forthcoming 2020).

[21] Chander et al., *supra* note 2, at 24–37.

https://doi.org/10.1017/aju.2019.83 Published online by Cambridge University Press

the management of information, such as notice, choice, access, integrity, and enforcement.[22] Despite similarities, the CCPA regulates a smaller set of companies than the GDPR, they have different enforcement mechanisms, the CCPA is designed for consumer protection (or the Hohfeldian liberty-right model), and the CCPA does not turn on lawful processing.[23] Furthermore, these scholars emphasize that different regulatory styles and legal backdrops will influence the implementation and evolution of the law.

Jack Balkin has theorized a system of fiduciary duties applicable to the processing of personal data, much like those duties that adhere to doctors, lawyers, and accountants.[24] The idea of information or data fiduciaries has been echoed in other scholarship (with some opposition[25]) and legislative proposals, including the 2019 New York Privacy Act introduced by New York Senator Kevin Thomas and the 2018 Data Care Act, proposed by U.S. Senator Brian Schatz.

Yet another nascent model is a tax on personal data. The Governor of California has hinted that California might develop a policy to make technology companies pay California residents a data dividend for the use of their personal data.[26]

Despite compelling arguments about EU influence, we have yet to see what shape the U.S. regime will take. Ultimately, the U.S. framework will sway many governments' approaches to privacy law. This has not escaped notice. In 2019, European Commissioner Vera Jourova said:

> I see two camps . . . a people-friendly camp that understands that we should have more control over our data . . . . Europe is a proud member of this club because it is based on our values . . . .
>
> And there is the other camp that has a lax approach to privacy . . . . I would want the US to join us in the first camp.[27]

Financial Interests

Companies have a financial interest in lobbying for less restrictive data protection regulations.[28] Ultimately, the benefits of GDPR-like regulation may not justify the cost of corporate compliance.

GDPR preimplementation spending neared US$7 billion for *Fortune* Global 500 companies, US$1 billion for FTSE 350 companies, and millions for medium-sized companies.[29] In a 2018 survey by Merrill Corp., 55 percent of respondents stated that deals they worked on fell apart because of concerns about a target company's compliance with GDPR.[30] According to a July 2019 poll conducted by the European Business Awards, almost 30 percent

[22] *Id.* at 14–15.

[23] *Id.* at 18–19.

[24] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183, 1205 (2016).

[25] *See, e.g.*, Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, Atlantic (Oct. 3, 2016); *see also* Barrett, *supra* note 18. *But see* Lina Khan & David Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497 (2019).

[26] *See* Jill Cowan, *How Much Is Your Data Worth?*, N.Y. Times (Mar. 25, 2019).

[27] European Commission, Press Release, Speech by European Commissioner Vera Jourova on the EU-US Digital Cooperation: A Common Response to Tech Challenges, Brookings Inst. (Apr. 11, 2019).

[28] Kartikay Mehrotra et al., *Google and Other Tech Firms Seek to Weaken Landmark California Data-Privacy Law*, L.A. Times (Sept. 4, 2019).

[29] *See* Daniel Castro & Michael McLaughlin, *The GDPR Will Make Your Online Experience Worse*, Fortune (May 23, 2018); Oliver Smith, *The GDPR Racket: Who's Making Money from This $9bn Business Shakedown*, Forbes (May 2, 2018); Tim Worstall, *Is GDPR Worth the Cost?*, ComputerWeekly (June 5, 2019).

[30] *See* Nina Trentmann, *Data Protection Concerns Upend M&A Plans*, Wall St. J. (Nov. 13, 2018).

https://doi.org/10.1017/aju.2019.83 Published online by Cambridge University Press

of European businesses admit to not being in compliance with GDPR.[31] On the other hand, as previously discussed, administrative fines have been relatively low.

Lobbying efforts to dilute the CCPA suggest that those companies singing the praises of GDPR will try to protect their bottom lines in the face of new legislation.[32] Furthermore, while U.S. legislators have more power to regulate tech companies, they may hesitate to do so because they need Silicon Valley "for job creation, economic growth, a buoyant stock market and, naturally, campaign contributions."[33]

The development of artificial intelligence (AI) is also a salient commercial consideration. EU data protection authorities have long recognized the need for attention to ethical data processing in the development of big data analytics and AI. Articles 13, 14, and 22 of GDPR directly address automated decision-making.[34] It is unclear whether the United States has the same resolve as the EU to create governing frameworks around the development of AI,[35] especially if it perceives that China is outstripping other world powers.[36] The Trump administration has said it supports the May 2019 non-binding Organisation for Economic Co-Operation and Development Principles on Artificial Intelligence, but lagging federal legislation and the President's 2019 AI Initiative suggests a desire to maintain an edge in AI innovation. America may decide to prioritize the development of AI over data subject privacy.

Will countries that are not home to major tech companies maintain GDPR-like data protection to secure market access to the EEA? Or will they eschew the GDPR in favor of allowing domestic industry to develop? In 2018, Bhaskar Chakravorti wrote that emerging markets are often overlooked and the GDPR "would impose costs on the mostly small businesses that operate in these regions . . . . [I]mposing a heavy burden on fledgling local data industries could stifle the chance for those companies to grow and compete."[37] Chakravorti is not alone.[38] But some jurisdictions may be following a GDPR-like approach. For example, the Council of Europe is actively encouraging African countries to accede to the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108), an international treaty aligned with GDPR principles via Convention 108 + .[39] So far, six African nations have signed on; further accession could indicate a growing appetite for European-style data protection regulation in that region.

Ultimately, companies in liberty-right-oriented jurisdictions are more likely to advocate commerce-friendly models of privacy and data protection regulation and liberty-right jurisdictions are more likely to listen.

Conclusion

A U.S. model, whatever that looks like, may prove as compelling as the current EU one: in many contexts, access to the U.S. market is at least as desirable as access to the EU market and many of the companies currently adopting

[31] *30% of European Businesses Are Still Not Compliant with GDPR*, RSM Global (July 22, 2019).

[32] Mahotra et al., *supra* note 28.

[33] Laurence Dodds & Olivia Rudgard, *Is Europe Winning the Argument on How to Regulate Big Tech?*, Telegraph (July 6, 2019).

[34] GDPR, *supra* note 5, arts. 22, 13, 14.

[35] *See* Forbes Insights with Intel AI, *Rethinking Privacy for the AI Era*, Forbes (Mar. 27, 2019).

[36] *See, e.g.*, Heather Long, *In Davos, U.S. Executives Warn that China Is Winning the AI Race*, Wash. Post (Jan. 23, 2019).

[37] Bhaskar Chakravorti, *Why the Rest of the World Can't Free Ride on Europe's GDPR Rules*, Harv. Bus. Rev. (Apr. 30, 2018).

[38] *See, e.g.*, Prashant Reddy T., *Should There Be a "Developing Country" Template for Data Protection Legislation?*, The Wire (May 17, 2018); Leonid Bershidsky, *Europe's Privacy Rules Are Having Unintended Consequences*, Bloomberg Opinion (Nov. 14, 2018); Jedidiah Yueh, *GDPR Will Make Big Tech Even Bigger*, Forbes (June 26, 2018).

[39] *See* Jennifer Baker, *What Does the Newly Signed "Convention 108+" mean for UK Adequacy?*, Int'l Ass'n of Privacy Professionals (Oct. 30, 2018).

https://doi.org/10.1017/aju.2019.83 Published online by Cambridge University Press

GDPR-compliance programs are also headquartered in, or targeting, the United States. They will have to negotiate between differently restrictive regimes, perhaps favoring one over the other for reasons of cost, efficacy, or values.

In 2018, I wrote that the GDPR may create a "Delaware effect" or a "California effect"—the regulatory shift toward or away from GDPR-like regulatory regimes.[40] In those early days, I assumed that the system was binary (a "race to the bottom or a race to the top"). After additional legislative and academic movement, and a year into the GDPR, regulatory innovation, differing privacy values, and practical considerations cast doubt on the universality of the GDPR model and make space for a new American norm.

[40] Shannon Togawa Mercer, *Sorting Through GDPR: What to Watch After May 25*, LAWFARE (May 25, 2018).

https://doi.org/10.1017/aju.2019.83 Published online by Cambridge University Press