doi:10.1017/aju.2019.79

SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

A TALE OF TWO PRIVACY LAWS: THE GDPR AND THE INTERNATIONAL RIGHT TO PRIVACY

Vivek Krishnamurthy[*]

The European Union's General Data Protection Regulation (GDPR)[1] is widely viewed as setting a new global standard for the protection of data privacy that is worthy of emulation,[2] even though the relationship between the GDPR and existing international legal protections for the right to privacy remain unexplored. Correspondingly, this essay examines the relationship between these two bodies of law, and finds that the GDPR's provisions are neither necessary nor sufficient to protect the right to privacy as enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[3] It argues that there are other equally valid and effective approaches that states can pursue to protect the right to privacy in an increasingly digital world, including the much-maligned American approach of regulating data privacy on a sectoral basis.

The Right to Privacy in International Law

As human rights go, privacy is relatively new. Samuel Warren and Louis Brandeis were the first to advance the notion that privacy is a right deserving of legal protection,[4] although the concept has antecedents in the doctrines of many different legal systems. Privacy is distinctive among the core civil and political rights, however, in that it was enshrined in international law before it was comprehensively guaranteed by any domestic constitutional system.[5] Prior to the adoption of the Universal Declaration of Human Rights (UDHR) in 1948,[6] domestic legal systems had only protected certain aspects of what we now consider the right to privacy. They did not include what Oliver Diggleman and Maria Cleis have called an "integral guarantee" of the right—that is, a comprehensive

* *Samuelson-Glushko Professor of Law, University of Ottawa; Senior Fellow, Carr Center for Human Rights Policy, Harvard University; Affiliate, Berkman Klein Center for Internet & Society, Harvard University.*

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

[2] *See, e.g.*, Věra Jourová, Eur. Commissioner for Just., Consumers, and Gender, What Next for European and Global Data Privacy?, Address Before the 9th Annual European Data Protection and Privacy Conference (Mar. 20, 2019) (describing the trend in numerous countries toward adopting "an overarching privacy law, with a core set of safeguards and rights, and enforced by an independent supervisory authority," patterned on the GDPR).

[3] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 UNTS 171 [hereinafter ICCPR].

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

[5] Oliver Digglemann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 441 (2014).

[6] Universal Declaration of Human Rights, Dec. 10, 1948, GA Res. 217 A (III) (1948).

recognition that the entire concept of "privacy" deserves protection. The *travaux préparatoires* of the UDHR, the ICCPR, and the European Convention on Human Rights[7] indicate that the right to privacy was included in all three instruments as an afterthought,[8] so there is little to be gleaned regarding the meaning of this right from the drafting history of these instruments.

Illumination as to the meaning of the right to privacy enshrined in Article 17 of the ICCPR[9] is most readily found in General Comment 16, which the UN Human Rights Committee adopted in 1988.[10] Given the pace of technological change over the last thirty years and the concomitant development of privacy law, it may seem odd to rely on such an old document to establish the meaning of Article 17. Be that as it may, General Comment 16 remains an appropriate starting point for interpreting Article 17, as it sets the expectations to which states are held when the Covenant's treaty body periodically assesses their implementation of Article 17.[11]

While most of the General Comment's eleven paragraphs focus on government searches, seizures, and surveillance,[12] there are two passages of particular significance to understanding the relationship between the ICCPR's guarantee of the right to privacy and the domestic data privacy laws that states have enacted in subsequent years.

First, the General Comment recognizes that the right to privacy "is required to be guaranteed against all [arbitrary or unlawful] interferences and attacks whether they emanate from State authorities or from natural or legal persons."[13] The Committee calls upon states "to adopt legislative and other measures to give effect to the prohibition against such interferences … as well as to the protection of this right."[14] The GDPR can be understood as one means by which EU member states guarantee certain aspects of the right to privacy against certain attacks by "State authorities or from natural or legal persons."

Second, General Comment No. 16 recognizes that:

> [t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, *must be regulated by law.* Effective measures have to be taken by States to ensure that *information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it,* and is never used for purposes incompatible with the Covenant.[15]

Taken together with the duty it imposes upon states to regulate by law "the gathering and holding of personal information on computers," General Comment 16 gives rise to an expectation that ICCPR states parties will enact data privacy legislation that binds both public and private actors.

[7] European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, E.T.S. No. 5 [hereinafter ECHR].

[8] Diggleman & Cleis, *supra* note 5, at 457.

[9] Article 17 of the ICCPR states:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks.

[10] Human Rights Committee, General Comment 16 (Thirty-second session, 1994), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, UN Doc. HRI\GEN\1\Rev.1 at 21 (1994) [hereinafter General Comment 16].

[11] *See generally* ICCPR, *supra* note 3, art. 40. *See also* Helen Keller & Leena Grover, *General Comments of the Human Rights Committee and their Legitimacy*, *in* UN Human Rights Treaty Bodies 129–30 (Helen Keller & Geir Ulfstein eds., 2012).

[12] General Comment 16, *supra* note 10, paras. 3–9.

[13] *Id.* at para. 1.

[14] *Id.*

[15] *Id.* at para. 10 (emphasis added).

"Neither Necessary Nor Sufficient"

Judged against this standard, the GDPR is neither necessary nor sufficient to protect the right to privacy against arbitrary and unlawful interference, as required by Article 17 of the ICCPR.[16] There are two reasons why it is insufficient. Article 2(1) of the GDPR specifies that it applies "to the processing of personal data wholly or partly by automated means," and to the processing by "other means" of data that forms or is intended to form part of a "filing system." As wide as this scope is, many aspects of the right to privacy fall outside the realm of data processing—such as searches and seizures of things and places in the physical world, or an individual's sexual and reproductive autonomy.[17] Correspondingly, the GDPR is but one tile in the mosaic of legal measures required of EU member states to adequately protect the right to privacy.

Even with regard to data privacy, however, there are exceptions to the GDPR's material scope that leave many kinds of data-intensive activities outside its purview. Specifically, GDPR Article 2(2) does not apply to data processing relating to activities that fall outside the scope of EU law, in the pursuit of the EU's common foreign and security policy, or in the context of criminal investigations and prosecutions. Needless to say, the (mis)use of personal data in the national security and law enforcement contexts has given rise to significant privacy-related controversies in recent years, yet this topic is entirely beyond the material scope of the GDPR. Correspondingly, the conformity of EU member states with Article 17 of the ICCPR requires looking beyond the GDPR even with regard to data-related privacy issues.[18]

Insofar as data processing activities fall within its material scope, the rules laid down by the GDPR conform with the expectations set forth in General Comment 16. For example, Article 4(1) defines personal data in the broadest imaginable terms, while Article 5 establishes that the processing of personal data must always be lawful, fair, and transparent. The consent of the data subject freely given will usually serve as the legal basis for the collection and processing of data, although the GDPR enumerates certain circumstances in which the processing of personal data is lawful absent consent. Article 15 establishes the right of data subjects to access their own data, while Articles 16–20 specify how and when data subjects can demand the correction or erasure of their data. Article 9, for its part, is noteworthy in prohibiting the processing of "sensitive" data that may reveal an individual's race, ethnicity, or sexual orientation (among other sensitive characteristics), unless one of a limited number of exceptions is met.

The GDPR certainly provides the strongest privacy protections of any law in the world today for those matters within its material scope. No comparable law endows individuals ("data subjects" in the GDPR's parlance) with such strong rights over data relating to them, and no other law imposes such strong conditions on the collection and use of personal data by private- and public-sector entities (data "controllers" and "processors" in the lingo). This is doubtless why privacy campaigners around the world have held up the GDPR as a model that their own jurisdictions should emulate.[19]

[16] Every EU member state has ratified the ICCPR. *See* U.N. Office of the High Commissioner of Human Rights, Status of Ratification Interactive Dashboard (choose "International Covenant on Civil and Political Rights" from the drop-down menu).

[17] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558, 564-55 (2003); A, B & C v. Ireland [GC], no. 25579/05, §§243–68, ECHR 2010-VI.

[18] The GDPR governs data processing activities by the EU and its member governments in all contexts other than those specifically excluded by Article 2(2).

[19] A notable example of this trend is privacy legislation introduced in Washington State earlier this year that was expressly modeled on the GDPR. Washington Privacy Act, H.B. 5376, Reg. Sess. (Wash. 2019). The legislation ultimately failed, however. *See* Lucas Ropek, *Why Did Washington State's Privacy Legislation Collapse?*, Gov. Tech. (Apr. 19, 2019). To be sure, the GDPR incentivizes other jurisdictions to adopt similar laws, inasmuch as Article 45 conditions transfers of Europeans' data to such jurisdictions only if the European Commission has determined that the jurisdictions to provide an "adequate level of protection" for such data.

Yet the GDPR's approach is neither sufficient on its own to comprehensively protect the right to privacy, nor a necessary means for states to meet their obligations under Article 17 of the ICCPR. The long-standing European approach to regulating data privacy might be ascendant worldwide,[20] yet it is just one means available to states to regulate "[t]he gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies."[21]

The American Approach to Privacy Regulation

This brings us to the venerable yet oft-critiqued American approach to regulating data privacy by sector. Instead of employing a single regulatory scheme to govern most public- and private-sector data processing, the United States has a bevy of federal and state laws governing data privacy in fields ranging from health[22] to education[23] to finance[24] to video rentals,[25] with decades-old consumer protection laws serving as a backstop against unfair and deceptive practices that negatively impact privacy.

While U.S. legal protections against government access to personal information are likely the strongest in the world,[26] American law has yet to adequately protect privacy against "interferences and attacks" that emanate from "natural or legal persons."[27] This may have begun to change with the passage of the California Consumer Privacy Act of 2018,[28] however, whose far-reaching data privacy protections have invited frequent comparisons with the GDPR.[29] In a recent paper that argues that the GDPR's role in inspiring the CCPA has been overstated,[30] Anupam Chander et al. find that the most salient difference between the two laws is that

> [t]he GDPR is built around the concept of "lawful processing" of data. That is, personal data cannot be processed unless a data controller has obtained individual consent, or the processing falls under one of the additional five listed categories of lawful processing. The CCPA does not require that processing be lawful. *Rather, it shares the presumption of most other American privacy law that personal data may be collected, used, or disclosed unless a specific legal rule forbids these activities.*[31]

This observation raises the question of whether the American approach to privacy law can be consistent with ICCPR Article 17, given that General Comment 16 suggests that "[t]he gathering and holding of personal information … *must be regulated by law.*" Can the U.S. approach sufficiently protect the right to privacy against attacks and

[20] Graham Greenleaf finds that 54 of the 120 data privacy laws in force around the world in 2017 are based on the model established in Europe by the GDPR and its predecessor, the EU Data Directive of 1995. *See* Graham Greenleaf, *Global Data Privacy Laws 2017*, 145 Privacy L. & Bus. Int'l. Rep. 10, 11–13 (2017).

[21] General Comment 16, *supra* note 10, para. 10.

[22] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191 (Aug. 21, 1996).

[23] Family Education Rights and Privacy Act of 1974, Pub. L. 90–247 (Aug. 21, 1974).

[24] Financial Services Modernization Act of 1999, Pub. L. 106–102 (Nov. 12, 1999) (widely known as the "Graham-Leach-Bliley Act" or GLBA).

[25] Video Privacy Protection Act of 1988, Pub. L. 100–618 (Nov. 5, 1988).

[26] Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 Emory L.J. 617 (2017).

[27] General Comment 16, *supra* note 10, para. 1.

[28] California Consumer Privacy Act of 2018, 2018 Cal. Stat. ch. 55. (A.B. 375).

[29] *See, e.g.*, Carol A.F. Umhoevfer & Tracy Shapiro, *CCPA vs. GDPR: The Same, Only Different*, DLA Piper (Apr. 11, 2019).

[30] Anupam Chander et al., *Catalyzing Privacy Law* 25–27 (U. Colorado Law Legal Studies Research Paper No. 19–25, 2019).

[31] *Id.* at 19 (emphasis added).

interferences by private entities, when its default position is that private information can be collected, used, and disclosed unless specifically forbidden by law? Or does ICCPR Article 17 require the comprehensive regulation of these activities *a la Européene,* subject only to certain enumerated exceptions?

The international legal authorities provide no clear answers to these questions, yet logic dictates that both the traditional European and American approaches to regulating privacy should be able to meet the standard set by Article 17. Regardless of whether the default position of the law is to permit or prohibit the collection and use of data in which individuals have privacy interests, a state can conform with Article 17 so long as its protections of this right are adequate when taken as a whole. Comprehensive coverage may be easier to achieve when the law presumes to regulate an entire field of activity subject to exceptions, rather than the other way around. Given the frequency with which exceptions swallow rules, however, thoughtful sectoral regulation *can* yield privacy protections that are stronger and better than an omnibus approach—as long as the resulting legal mosaic covers enough area.

Furthermore, there is more to law than just legislation. The American tradition of "adversarial legalism" leaves much to be sorted out by the courts—particularly through the development of tort law.[32] It would be a mistake, therefore, to equate the state of privacy law in the United States with the rules that are currently on the books, as the common law of privacy is capable of developing over time.[33] Indeed, courts took the initiative in developing the law of privacy in the United States following the publication of Warren and Brandeis's landmark article,[34] and the possibility remains open as the country grapples with the inadequacy of its current privacy laws.

Conclusion

Just as the GDPR is far from the final word on privacy in Europe, the American approach to regulating privacy may yet yield a level of protection for this right against public and private "interferences and attacks" that meets the high standard set forth by the ICCPR. It is possible that the United States might never get there, but there is no reason in principle why the country cannot do so through the pursuit of its own distinctive approach to regulating privacy.

[32] *See* Robert A. Kagan, Adversarial Legalism (2003), especially chapter 7.

[33] Were it to be adopted by the courts, Jack Balkin's notion that large internet platforms should owe fiduciary duties to their users would be an example of how a hoary common law doctrine could be used to ensure that "information concerning a person's private life … is never used for purposes incompatible with the Covenant," as General Comment 16 advises. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2006).

[34] Irwin R. Kramer, *The Birth of Privacy Law: A Century Since Warren and Brandeis*, 39 Cath. U. L. Rev. 703, 715–19 (1990).