doi:10.1017/aju.2019.82

# INTRODUCTION TO THE SYMPOSIUM ON THE GDPR AND INTERNATIONAL LAW

*Gráinne de Búrca*[*]

It is rare that a lengthy and detailed piece of legislation adopted in one jurisdiction becomes not only a law with powerful impact across multiple jurisdictions and continents, but also an acronym that trips readily off the tongue of laypeople and lawyers alike around the world. Yet this has been the fate of the European Union's General Data Protection Regulation, now commonly known as the GDPR, since its coming into force in 2018.

Perhaps the Helms-Burton Act came somewhat close in its global impact when the United States adopted the extensive anti-Cuba sanctions regime in 1996. But Helms-Burton was a deliberately globally-targeted sanctions regime that sought to pressure foreign companies trading in or with Cuba into ceasing those activities, and it was adopted as an instrument of U.S. foreign policy. By comparison, the GDPR at first glance appears to be a domestically-focused piece of legislation intended to strengthen data protection and privacy standards within the EU, and to make Europe, in the terms used by the European Commission, "fit for the digital age." Describing itself as a measure intended to harmonize data privacy laws across Europe's single market, the GDPR—which in principle requires no transposition on the part of EU member states in order to have immediate and binding legal effect within those states—applies to any organization operating within the EU or offering goods or services to customers or businesses in the EU. The legislation imposes a demanding set of regulatory standards on those who control or process personal data, in relation to the purposes, uses, handling, and storage of such data. Breaches of these standards can result in the imposition of hefty fines. While the overriding purpose of the regulation may be the protection of personal privacy, the GDPR addresses multiple aspects of data governance that are relevant to businesses worldwide.

The key to the way in which the GDPR goes far beyond being a domestic EU-focused legislative measure is in its application to any business or organization *anywhere in the world* that offers goods or services to persons within the EU, or that monitors the behavior of individuals in the EU. This has meant that the numerous and detailed regulatory standards imposed on companies and organizations—which include the need to obtain the affirmative consent of those whose data they gather or hold; the requirement to inform; the obligation to rectify and to erase data; and restrictions on transfers of data outside the EU—have a very extensive global reach indeed. As Anu Bradford has convincingly argued, at a time when the EU has emerged from a series of economic and political crises as a weakened international political actor, its global regulatory influence and power by comparison has, if anything, increased.[1] While some have welcomed the EU's digital leadership in setting strong data protection and privacy standards, others have been critical of the reach and implications of the GDPR, with the Heritage Foundation and others accusing the EU of digital imperialism.[2] One evident consequence of the global impact of the GDPR is that many of its requirements are in tension with, if not directly in conflict with, other regimes and

* *Florence Ellinwood Allen Professor of Law, New York University.*

[1] Anu Bradford, The Brussels Effect: How the European Union Rules the World (forthcoming 2020).

[2] Theodore Bromund, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*, Heritage Found. (Jan. 9, 2018).

principles of international law, and compliance with the GDPR could well lead companies and organizations into violation of other legal and regulatory obligations.

The six essays in this symposium address several of these tensions and conflicts. Cedric Ryngaert and Mistale Taylor of Utrecht University open the symposium with a discussion of the compatibility of the global reach of the GDPR with the principles of jurisdiction under customary international law.[3] They argue that the GDPR's scope is compatible both with the principle of territorial jurisdiction and with the "passive personality" principle of international law. However, they go beyond this to argue that the extraterritorial scope of the GDPR is not only permitted under international law but could even be said to be required under EU law by the EU's recognition of data protection as a fundamental right of its residents. Nevertheless, being compatible with international law principles of jurisdiction and required by EU data protection principles does not mean that the GDPR does not create tension with other countries that may have even stronger jurisdictional grounds to regulate protection of the same data. The authors, however, note the absence of general pushback from other states so far against the extraterritorial application of the GDPR, but caution that this does not necessarily mean that there are no objections to it, and more importantly, that it does not answer the normative question as to whether the EU *should* aggressively extend the reach of its data protection standards.

In their essay on the compatibility of the GDPR's restrictions on data transfer out of the EU with the nondiscrimination rules of the General Agreement on Trade in Services (GATS), Svetlana Yakovleva and Kristina Irion of the University of Amsterdam similarly emphasize how EU law has—through the EU Charter on Fundamental Rights as well as through legislation—created a fundamental right to data protection.[4] They argue that the GDPR's requirement of an EU "adequacy finding" before data can be transferred out of the EU probably does not fall within the exception in the GATS for data protection since it is not the "least trade restrictive" means available for protecting data in the event of transfer. At the same time, the authors suggest, the adequacy requirement is probably the only way of properly guaranteeing the EU's fundamental right to data protection. How should the EU navigate such a conflict between its commitment to this fundamental right and its commitment to the rules of international trade? Yakovleva and Irion suggest that an intimation of the EU's approach is to be found in its recent negotiating position on digital trade and cross-border data flows, where it sought a more broadly worded and flexible exception for data protection that would be similar to the national security exception currently contained in the GATS. The problem with this approach, however, is that it puts the EU at odds with the United States on digital data flows, and makes it harder for the two transatlantic powers to agree on a common position that could strengthen their negotiations with authoritarian states such as China and Russia.

The Vrije Universiteit Brussel's Christopher Kuner then addresses whether the GDPR applies to international organizations.[5] This question is left uncertain by the terms of the GDPR itself, and the EU has not fully clarified its stance on the issue. It is an issue that matters a great deal to many international organizations, not least because international organizations based outside Europe regularly seek personal data from companies such as Facebook, Google, or LinkedIn, which are subject to the GDPR. Kuner points to the arguments that support the view that international organizations are subject to the GDPR as well as those that oppose that view, and discusses whether the EU should respect the privileges and immunities granted by its member states to international organizations. He notes that while international organizations are unlikely to find themselves subject to "hard" enforcement of the GDPR, nevertheless they could find themselves facing other incentives and softer forms of enforcement pressure. Kuner concludes by arguing that international organizations—given the importance to so many of them of

[3] Cedric Ryngaert & Mistale Taylor, *The GDPR as* Global *Data Protection Regulation?*, 114 AJIL UNBOUND 5 (2020).

[4] Svetlana Yakovleva & Kristina Irion, *Toward Compatibility of the EU Trade Policy with the General Data Protection Regulation*, 114 AJIL UNBOUND 10 (2020).

[5] Christopher Kuner, *The GDPR and International Organizations*, 114 AJIL UNBOUND 15 (2020).

https://doi.org/10.1017/aju.2019.82 Published online by Cambridge University Press

digital data—would be wise to implement the standards contained in the GDPR as best practices, whether or not they consider themselves legally bound to do so, and he argues for greater dialogue and bridge-building between the EU and international organizations on issues such as data protection and transfer.

Shannon Togawa Mercer, an attorney at Skadden, returns to the theme of the GDPR's global reach, and asks whether the Regulation is either viable or desirable as a global standard.[6] She notes that despite how it has dominated the global conversation and influenced the adoption of similar laws in many parts of the world, the efficacy of the GDPR has not in fact been proven, given how few enforcement actions have so far been taken. She argues that the U.S. system—including the California Consumer Protection Act—is developing an alternative and quite different set of standards with fundamentally different assumptions about the right to privacy, and that the corporate cost of complying with the EU's standards means that it is unlikely to be attractive to countries that prioritize commercial freedom over stringent privacy protection. Mercer also questions whether the GDPR is suitable for emerging and developing economies given the costs it would entail for fledgling local data industries. She concludes by calling into question the universality of the GDPR model and argues that there is room for a different U.S.-style norm.

The final two essays examine the relationship and the potential tension between the GDPR and different aspects of international human rights law. Vivek Krishnamurthy of the University of Ottawa considers the relationship between the right to privacy implicit in the GDPR and the right to privacy under international human rights law, while the Digital Freedom Fund's Nani Jansen Reventlow addresses the tension between the provisions of the GDPR and freedom of expression.

Echoing Shannon Mercer's argument that the U.S. approach to data protection may be preferable, for many businesses and economies, to that of the EU, Krishnamurthy argues that there are many approaches to the regulation of data privacy—including the sectoral approach of the United States—that could be preferable to or at least as valid as the approach embodied in the GDPR.[7] He examines the protection of the right to privacy under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights (ICCPR), and the European Convention on Human Rights, and concludes that the degree of protection for the right to privacy provided by the GDPR is neither necessary nor sufficient for compliance with international human rights law. It is not sufficient because the GDPR covers only data processing and because of the many exceptions to the material scope of the EU Regulation, and it is not necessary because there are other ways of satisfying the privacy requirements of international human rights law. Krishnamurthy argues that both the comprehensive approach adopted by the GDPR (within its material scope) and the sectoral approach adopted by the United States to the protection of privacy should—at least in principle—be consistent with the requirements of Article 17 of the ICCPR on the right to privacy.

Finally, Nani Jansen Reventlow explores the implications of the GDPR for freedom of expression, and particularly for the activity of journalists.[8] She argues that while privacy is well-protected under the EU Regulation, far less attention has been given to protection for freedom of expression and that as matters stand, there is a risk that the provisions of the GDPR could compromise freedom of the press. She cautions that data protection laws could be weaponized—just as libel laws have been in the past—to threaten or silence news stories that rely on or include personal data, and she points to some examples of this already arising in Europe. Despite the inclusion of a provision in the GDPR requiring EU member states to reconcile data protection with freedom of expression, which explicitly mentions processing for journalistic purposes, Jansen Reventlow notes that while virtually all EU states

[6] Shannon Togawa Mercer, *The Limitations of European Data Protection as a Model for Global Privacy Regulation*, 114 AJIL Unbound 20 (2020).

[7] Vivek Krishnamurthy, *A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy*, 114 AJIL Unbound 26 (2020).

[8] Nani Jansen Reventlow, *Can the GDPR and Freedom of Expression Coexist?*, 114 AJIL Unbound 31 (2020).

https://doi.org/10.1017/aju.2019.82 Published online by Cambridge University Press

have already implemented the protections for privacy required by the Regulation, the same is not true for the adoption of legislation to implement the journalistic exception. She indicates that many states have not introduced laws creating an exception for journalism, and those that have been introduced are uneven in their protection, with some being excessively vague and others contradictory.

All of the essays in the symposium point both to the influential nature of the GDPR as a European as well as global data protection law, and to some of the problems, uncertainties, costs, and tensions it has created for organizations, businesses, journalists, and others. Less than two years after its entry into force, many questions still remain to be resolved through practice. What is without question, however, is that the enactment of the GDPR as a regional data protection law has had significant worldwide ramifications, including tensions with other international legal regimes. It remains to be seen whether the GDPR does indeed become a global data protection standard or whether, as several of the authors in this symposium suggest, it will soon be rivalled by other regulatory approaches that offer different options to states and businesses around the world.

https://doi.org/10.1017/aju.2019.82 Published online by Cambridge University Press