*This is an Accepted Manuscript of a book chapter published in Federico Fabbrini, Edoardo Celeste and John Quinn (eds), Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty (Hart 2021),*
*https://www.bloomsburyprofessional.com/uk/data-protection-beyond-borders-9781509940677/*

# Introduction

Federico Fabbrini, Edoardo Celeste, and John Quinn

The purpose of this book is to examine the protection of personal data from a transatlantic perspective. Personal data are the backbone of the contemporary digital society. Data, by its nature, is a-territorial, yet law has traditionally been limited by territorial boundaries. Therefore, a tension emerges between data and the laws which regulate it. As a result of this tension, a serious question has emerged regarding how to protect personal data rights across borders. Data flows across jurisdictions for commercial purposes, as digital companies transfer data from subsidiaries to the headquarters for processing purposes. Moreover, data flow occurs in the context of law enforcement, as national authorities increasingly seek access to personal data stored in foreign countries in order to prevent and fight serious crimes. The issues that arise from this situation have been mostly developed in the transatlantic context between the European Union (EU) and the United States (US), which are at the vanguard of technological innovation.

Over the past few years, both sides of the Atlantic have been characterised by significant legislative and jurisprudential developments in the field of data privacy. In 2016, the EU adopted a new pan-European data protection law – the General Data Protection Regulation (GDPR)[1] – while, in the US, at state level, California passed a new data privacy legislation,[2] and, at federal level, the CLOUD Act has introduced the possibility for law enforcement authorities to request data stored in third countries.[3] In both jurisdictions, moreover, seminal judicial decisions have been recently adopted, such as judgments by the EU Court of Justice (CJEU) involving the American tech giants Facebook[4] and Google,[5] and the much-discussed US Supreme Court *Carpenter* case, which applies constitutional protections against law enforcement agencies accessing cell location data.[6] These developments have produced, on occasion, convergence and cooperation between the two regimes, but on other, also amplified pre-existing areas of

[1] Regulation (EU) 2016/679, OJ 2016 L 119/1.

[2] California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.100-.199 (West 2018) (effective Jan. 1, 2020).

[3] Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 1625, 115th Cong. div. V (2018).

[4] Case C-18/18, *Eva Glawischnig-Piesczek v. Facebook Ireland Ltd.* [2019]

[5] Case C-507/17, *Google LLC v Commission Nationale de l'Informatique et des Libertés* (CNIL) [2019].

[6] *Carpenter v. United States*, 138 S.Ct. 2206, 2220 (2018).

tensions. The recent July 2020 CJEU judgment in *Schrems II*,[7] declaring invalid the EU Commission decision establishing the adequacy of the EU-US Privacy Shield, is a paradigmatic example of how, after years of intense debate and failed reforms, there is still a significant divergence between the EU and the US in the field of data privacy.

These developments, as this book explains, are further complicated by the emergence of two conflicting dynamics in the digital environment. On the one hand, on both sides of the Atlantic and beyond, jurisdictions increasingly endeavour to apply their legislation extraterritorially. In particular, the EU applies data protection law outside its borders in order to ensure an effective protection of European fundamental rights and limit the risk of circumvention. The US, instead, have recently adopted new legislation to access data stored in foreign data centres managed by US-based companies. On the other hand, both jurisdictions also endeavour to claim, with ever greater assertiveness, their sovereignty over data and digital infrastructures. The EU is investing significantly in a project to build a cloud 'made in the EU' that could compete against the American tech giants. The US, as a response, are considering strengthening their position by adopting a competing federal legislation, which would favour business and foster innovation.

These trends are further blurred by fast-changing technological changes and by the fluidity of longer-term processes that are currently subverting pre-existing economic and political equilibria. In particular, Brexit – the United Kingdom (UK) withdrawal from the EU – will change the status of the UK from EU member state, towards which data can be freely transferred, to third country, which will require specific arrangements similar to those that the European Commission is since years attempting to put in place with the US. In parallel, the increasing EU quest for digital sovereignty, which seeks to reattract data in the orbit of the EU, clashes with the technological superiority of US technology companies, and risks to generate a counterproductive arm-wrestling in a context already in turmoil because of the economic war currently under way between the US and China.

This book therefore aims to analyse these ongoing dynamics, shedding light on the EU and US developments in the field of data protection, the areas of tensions and cooperation between these jurisdictions, and the future prospects for the protection of data across borders.

The book, which brings together contributions by leading legal scholars from across Europe and the US, is structured in four parts. Part I sets the scene, presenting the latest legal developments in the field of data protection both in the EU and the US. Part II critically examines the emerging tensions in the protection of personal data beyond borders and analyses recent judgments dealing with issues of extraterritorial application of EU data protection law and their challenges. Part III analyses a series of scenarios where transatlantic cooperation in the data protection field is already present or advocated, with a particular focus on the law enforcement sector. Finally, Part IV reflects on the future prospects of the tension between extraterritoriality and sovereignty in the data protection field.

In Chapter 2, Edoardo Celeste and Federico Fabbrini map the legal architecture for the protection of personal data in the EU, examine its resilience in the context of Covid-19 and explore the question of the extraterritorial application of EU data protection law. The chapter explains that there are good arguments for the EU to apply its high data protection

[7] Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Schrems* [2020].

standards outside its borders. As data is un-territorial, only a global application of EU data protection law can guarantee an effective enforcement of privacy rights. However, the chapter also highlights how such an extraterritorial application of EU data protection law faces challenges, as it may clash with duties of international comity and the need to respect diversity of legal systems, and could ultimately be nullified by contrasting rulings delivered by other courts in other jurisdictions. As the chapter points out from a comparative perspective, the protection of privacy in the digital age increasingly exposes a tension between efforts by legal systems to impose their high standards of data protection outside their borders and claims by other legal systems to assert their own power over data. The chapter suggests that navigating these conflicting currents will not be an easy task, and that greater convergence in the data protection framework of liberal democratic systems worldwide appears as the preferable – albeit far from easy – path to secure privacy in the digital age.

In Chapter 3, Jordan Fischer investigates the US data privacy legal framework. She argues that, in contrast to the EU, the US adopted a radically different approach in the privacy field. The right to privacy was never enshrined in the Constitution, but progressively recognised by the case law of state and federal courts. US data privacy legislation is sectoral and fragmented. Industry codes and standards play a significant role. Fischer contends that, despite the echo that the GDPR has exercised over the past few years, the US can still provide a crucial input to frame a global approach to privacy. The chapter explores how the US can develop a new federal legislation, while resisting the GDPR effect and preserving the peculiarities of the US tradition. In particular, Fischer argues that a new federal privacy legislation should still rely on the mix of public authorities' oversight and private companies' self-enforcement that is common in the US. The chapter finally explains how developing a new federal privacy framework in the US presents a series of challenges, but also offers multiple opportunities.

In Chapter 4, John Quinn analyses the 2019 CJEU decision in *Google v CNIL*, which directly addressed the territorial scope of a successful dereferencing request made under the right to be forgotten in Article 17 of the GDPR, and discusses the implications of this major case. The CJEU held that that the default position of EU law was that search engines, following a successful dereference request, must remove the relevant information on their EU domains only, and not across all versions of their search engine. Therefore, the case limited the territorial scope of a successful de-referencing request to within the EU. Quinn explains how the existence of geo-blocking technology influenced the ruling of the CJEU. However, he contends that, because the right to be forgotten is not absolute, the CJEU decision in *Google v CNIL* is a proportionate one in attempting to balance rights on a global scale.

In Chapter 5, Dana Burchardt examines tensions within the EU by analysing the German Federal Constitutional Court's recent jurisprudence on the right to be forgotten. In two decisions delivered in late 2019, the Constitutional Court developed a framework of "parallel applicability" which seems to reduce the scope of application of EU fundamental rights in Germany. The framework also allows the German Court to influence how the right to be forgotten under EU law is interpreted and applied within the German legal order. Burchardt argues that the framework significantly broadens the competence of the German Constitutional Court thereby creating a significant risk of internal fragmentation in the protections offered by EU law as well as inconsistencies due to a diverging EU and German interpretation of EU law, in the data protection field and beyond.

In Chapter 6, Oreste Pollicino offers a comprehensive overview of the effects of the extraterritoriality of EU law, investigating to what extent the case law of the CJEU in the digital field has an impact on the digital sovereignty of third states. The chapter claims that the CJEU has turned privacy and data protection into a 'super' fundamental right and that this constitutes the theoretical justification for the extraterritorial effects of the EU legal system. Pollicino argues that the absence of a comprehensive privacy framework in the US, combined with the special status that EU legislation and case law have accorded to the rights to privacy and data protection, has fuelled a process of 'Europeanisation' at global level. The chapter analyses as further example of this trend the recent CJEU decision in *Glawischnig-Piesczek v. Facebook*, illustrating how the CJEU is explicitly authorising a global application of EU law, if necessary to preserve European fundamental rights.

In Chapter 7, Maria Tzanou addresses the conditions on which the extraterritorial effects of EU law are grounded, focusing on the application of EU fundamental privacy rights to transborder data flows. She analyses the *Schrems I* decision where the CJEU invalidated the EU administrative framework for data transfers to the US as incompatible with EU fundamental rights. She also analyses the July 2020 judgment of the CJEU in *Schrems II* where again the CJEU ruled to suspend the transfer of his personal data from Facebook Ireland to its US mother company, on the basis that the data could be made available to American authorities in violation to EU privacy rights. She argues that the CJEU has failed to consider important theoretical and doctrinal considerations in these decisions and has neglected to meaningfully engage with the interpretation of EU fundamental rights in the context of their extraterritorial application.

In Chapter 8, Stephen Smith examines the CLOUD Act, a US federal statute which provides law enforcement authorities significant power to obtain electronic data stored in foreign jurisdictions. Smith focuses on the provisions which authorise real-time surveillance of the activities of criminal suspects and others beyond US territory. He outlines the modes of surveillance explicitly and implicitly covered by the CLOUD Act and explains their potential extraterritorial impacts. One of Smith's concerns is that much of the Act contains ambiguous language that perhaps implicitly authorises numerous types of surveillance, including 'network investigative techniques', a term Smith believes to equivalent to hacking. Smith explores the implications of this piece of US legislation in the context of international law and argues that to the extent the CLOUD Act authorises US law enforcement to unilaterally engage in surveillance on foreign soil, it disregards international law.

In Chapter 9, TJ McIntyre analyses the system of voluntary disclosure by Irish-based online service providers to foreign law enforcement authorities. The chapter explains that digital companies established in the jurisdiction of the Irish state play a crucial role, by acting as controllers of the data of millions of European users. McIntyre argues that, despite this responsibility, the Irish state did not ratify the Cybercrime Convention and failed to regulate cross-border access to data stored in Ireland. By virtue of vague provisions of Irish law, foreign law enforcement authorities regularly resort to companies based in Ireland to request personal data that otherwise could be obtained only through the lengthy and burdensome mutual legal assistance procedure. McIntyre argues that this practice has been made illegal by the entry into force of the GDPR, and shows that this circumstance may be regarded as a violation of the obligations owed by the Irish state by virtue of the ECHR, and considers option to challenge the status quo.

In Chapter 10, Angela Aguinaldo and Paul De Hert critically assess the last decade of direct cooperation, this time, between EU law enforcement authorities and US technology companies. The chapter reconstructs the legal grounds justifying the use of direct transatlantic cooperation in the law enforcement context, and analyses the new opportunities offered by the adoption of the US CLOUD act and a series of proposal at European level, including the additional protocol to the Cybercrime Convention and the EU e-evidence package. Aguinaldo and De Hert highlight the persistence of a series of public international law conundrums related to sovereignty and jurisdiction and the risks deriving from a burden shift from public authorities to private companies. The chapter concludes by analyzing to what extent the new direct cooperation systems still fail to address significant data protection issues, and by highlighting the relevance of the recent *Schrems II* CJEU decision and the judgment of the German Federal Constitutional Court on the proportionality of domestic production orders in this field.

In Chapter 11, Vincenzo Zeno-Zencovich investigates whether international trade law could be a solution to avoid conflicts of law and guarantee free-flow of data across borders. The chapter illustrates the complexities of applying international trade law to data flows. It highlights that data exchanges are not easily classifiable as either goods or services, often because they represent ancillary elements of a transaction. It critically appraises to what extent the same notion of data, and in particular those of personal nature, may fit with the rules of international trade. Zeno-Zencovich explains that the international trade law principles of the 'Most Favoured Nation' (MFN) and 'National Treatment (NT) do not offer practical solutions, when applied in the context of data flows. As such, Zeno-Zencovich concludes by exploring alternative answers to the application of these international trade law principles, and illustrating potential fora that could successfully address the issue of free-flow of data.

In Chapter 12, Orla Lynskey critically addresses the mechanisms through which EU law gains its extraterritorial effects. Firstly, by comparing EU data protection law with other areas of EU law, she argues that extraterritorial impact is not particular to EU data protection law thereby rejecting claims of data exceptionalism. As she points out, environmental law, and competition law are other examples where EU law operates beyond its borders. Lynskey then continues examining the rationale for EU law's extraterritorial impact, arguing that it flows from nascent principles of EU law such as mutual trust and the autonomy of the EU legal order. Finally, she concludes using the question of cross-border data flows after Brexit to support the argument for the extraterritorial effect of EU law.

In Chapter 13, finally, Edoardo Celeste reconstructs the meaning of digital sovereignty, investigating its significance, rationale and challenges as a core value inspiring recent policy in the EU. The chapter overviews the historical evolution of the concept of sovereignty in general, and contextualises its application in the digital ecosystem, providing a definition of 'digital sovereignty'. Celeste then examines how this concept has been articulated in the EU, explaining that the rationale underlying this idea lies in the need to preserve the European DNA of values and rights. European data are mostly processed by foreign companies and stored outside the EU. This circumstance poses serious risks in terms of potential fundamental rights violations. The chapter therefore summarizes a number of initiatives that have been put forward to strengthen the EU digital sovereignty. However, Celeste also illustrates a series of risks associated with this tendency, warning that digital sovereignty can easily degenerate into forms of

sovereigntism. Celeste finally contends that EU rights and values can continue to be uphold without resorting to a counterproductive arm-wrestling with foreign countries, by respecting the principles of international comity, peacefully cooperating and respecting pluralism.

Indeed, as the recent Covid-19 pandemic has pointed out, borders remain a porous concept, and cooperation trumps isolation as the way to deal with transnational problems like a pandemic. Yet, as this book explains, with specific reference to data, the protection of privacy across borders remains a work in progress – and we hope that this collective volume will contribute to the debate on how to advance in this effort, particularly in a transatlantic context.