ECONSTOR
*Make Your Publications Visible.*

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Gstrein, Oskar Josef; Zwitter, Andrej Janko

**Article**

# Extraterritorial application of the GDPR: Promoting European values or power?

Internet Policy Review

**Provided in Cooperation with:**
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

*Suggested Citation:* Gstrein, Oskar Josef; Zwitter, Andrej Janko (2021) : Extraterritorial application of the GDPR: Promoting European values or power?, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 10, Iss. 3, pp. 1-30, https://doi.org/10.14763/2021.3.1576

This Version is available at:
https://hdl.handle.net/10419/245340

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*

https://creativecommons.org/licenses/by/3.0/de/legalcode

WWW.ECONSTOR.EU

Mitglied der Leibniz-Gemeinschaft

INTERNET POLICY REVIEW
Journal on internet regulation

**Volume** 10 **Issue** 3

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

# Extraterritorial application of the GDPR: promoting European values or power?

**Oskar Josef Gstrein** *University of Groningen* o.j.gstrein@rug.nl
**Andrej Janko Zwitter** *University of Groningen*

**DOI:** https://doi.org/10.14763/2021.3.1576

**Published:** 30 September 2021
**Received:** 12 November 2020 **Accepted:** 31 March 2021

**Competing Interests:** The author has declared that no competing interests exist that have influenced the text.
**Licence:** This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. https://creativecommons.org/licenses/by/3.0/de/deed.en
Copyright remains with the author(s).

**Citation:** Gstrein, O. J. & Zwitter, A. J. (2021). Extraterritorial application of the GDPR: promoting European values or power?. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1576

**Keywords:** European values, GDPR, Privacy, Extraterritoriality

**Abstract:** This article examines whether the territorial scope of the EU General Data Protection Regulation promotes European values. While the regulation received international attention, it remains questionable whether provisions with extraterritorial effect support a power-based approach or a value-driven strategy. Developments around the enforceability of a 'right to be forgotten', or the difficulties in regulating transatlantic data flows, raise doubts as to whether unilateral standard setting does justice to the plurality and complexity of the digital sphere. We conclude that extraterritorial application of EU data protection law currently adopts a power-based approach which does not promote European values sustainably. Rather, it evokes wrong expectations about the universality of individual rights.

## Section 1. Introduction

In the recent history of the European Union (EU) few legislative acts gained as much attention as the 2016 General Data Protection Regulation (GDPR; Kantar, 2019). Pursuant to Article 97 GDPR, the EU Commission published an evaluation of the regulation on 24 June 2020, in which it states: 'The GDPR has already emerged as a key reference point at international level and acted as a catalyst for many countries around the world to consider introducing modern privacy rules. This trend towards global convergence is a very positive development that brings new opportunities to better protect individuals in the EU when their data is transferred abroad while, at the same time, facilitating dataflows' (European Commission, 2020a, p. 12).

On the one hand, the regulation has been hailed as the new global 'gold standard' (Rustad & Koenig, 2019, p. 366). On the other hand, the attention it receives is surprising when considering the substantive provisions of GDPR in the larger context of the historic development of data protection law (Hoofnagle et al., 2019, pp. 69–72; Rustad & Koenig, 2019, pp. 368–369). Core principles and requirements such as Article 5 and 6 GDPR are only incremental improvements of what was already established across many European countries in the 1970s and 1980s (Ukrow, 2018, pp. 239–247). Certainly, some novel elements such as a 'right to be forgotten' (RTBF; Article 17 GDPR), a right to data portability (Article 20 GDPR), or the requirement for mechanisms to mitigate risks of automated individual decision-making ('artificial intelligence'; Article 22 GDPR) are innovative. However, it is precisely these provisions that require more detailed interpretation by courts and national data protection authorities via the European Data Protection Board (EDPB). Additionally, the precise interpretation of these rights is subject to intensive academic discourse and scrutiny (see e.g. Wachter et al., 2017).

Combining the arguments that the core principles of GDPR are well known and that the innovative elements require better understanding, one might conclude that it is probably not the substantive dimension of the regulation that explains its impact (Hoofnagle et al., 2019, pp. 66, 97). Rather, it seems that procedural and architectural elements of the framework require attention (Rojszczak, 2020, pp. 31–34). From an intra-EU perspective, the establishment of the GDPR marks a shift towards almost fully harmonised European law, which entails direct effects for the individual ('data subject'). In other words, the role of member states when it comes to the interpretation of provisions is being limited with more centralisation (European Data Protection Board, 2018, p. 4). In contrast, the emergence of this 'unified block' also has consequences for actors outside the EU, especially since the regula-

tion contains, with Article 3, a provision on territorial scope with considerable extraterritorial effect (de Hert & Czerniawski, 2016, pp. 236–240).

This contribution analyses central provisions and mechanisms of the GDPR that result in the extraterritorial effect of the framework. This includes Article 3 of the GDPR, as well as the legal regime that enables the European Commission to establish whether personal data is 'adequately protected' in other countries of the world. We investigate whether internal unification combined with extraterritorial reach is beneficial for the promotion of European values in data flows inside and outside the EU in the longer term. While scholars have already started to speculate about the effects of extraterritorial application before the applicability of the GDPR (de Hert & Czerniawski, 2016, p. 230), recent European and national jurisprudence on the RTBF (Gstrein, 2020, pp. 136–139) as well as criticism of the seeming lack of rigour of the Irish data protection authority to enforce European values in cross-Atlantic relations—as highlighted by the Court of Justice in '*Schrems II*' (Tracol, 2020)—raise the question whether the extraterritorial effect is not factually overburdening citizens and businesses as well as public institutions and political actors.

Considering options for a better future with high and effective data protection standards, we suggest that rather than relying on extraterritorial effect that adopts a power-based approach using the 'Brussels Effect', the universal protection and promotion of European values will be more sustainable when adopting value-based strategies. These could manifest in enhanced cooperation and traditional harmonisation of legal frameworks, with the objective to build broader international consensus around central regulatory principles, institutional requirements, as well as effective safeguards and remedies for those affected by the abuse of personal data. Certainly, some will doubt whether European data protection standards have the potential to form the basis for a broader multilateral agreement. Nevertheless, comparative research already shows that most of the 145 national frameworks around the globe regulating privacy and data protection at the end of 2020 apply the principle-based and technology neutral 'omnibus model', replicating the distinctive essence of European data protection laws in their respective legal systems (Greenleaf, 2021a). In other words, while the extraterritorial effect of GDPR is only effective since 2018, countries around the world have already started much earlier to enact and upgrade national laws to mirror what is 'arguably the world's best practice' (Greenleaf, 2021a, p. 5).

Therefore, in the area of data protection it might be best for the promotion of European values if the EU continues to develop and deliver high standards, while ac-

tively engaging in international fora and multilateral exchange—as long and as far as this opens venues to establish value-based governance frameworks. At the same time, effective and comprehensive enforcement of existing provisions on member states territories is important to maintain credibility. In conclusion, we argue that extraterritorial application of European data protection law is not a preferable strategy to promote European values sustainably. Rather, it evokes wrong expectations about the universality and enforceability of individual rights.

## Section 2. The 'Brussels Effect' and European values

In 2012 Anu Bradford introduced the concept of the 'Brussels Effect', which describes 'Europe's unilateral power to regulate global markets' (Bradford, 2012, p. 3). She argues that any political actor able to leverage and combine the five factors of market size, regulatory capacity, stringent standards (e.g. consistent approach to data protection), inelastic targets (e.g. non-mobile consumers), and non-divisibility (e.g. mass-production cost advantage for manufacturers and service providers) will be able to set the global regulatory standard for a certain regulatory area. According to her theory, the EU was able to increasingly establish such standards since the 1990s and therefore has become the 'global regulatory hegemon' (Bradford, 2020, pp. 25, 64). In simple terms, most global corporations adopt the European requirements for designing their products and services since this allows them to stick to a single regulatory regime. Even if this regime requires more costly adjustments compared to others, producers prefer the EU model since it enables them to operate and refine only one mode of production that is globally accepted. Therefore, products and services designed to comply with EU standards can be marketed globally.

According to Bradford's studies, examples of areas where the effect can be witnessed include market competition, consumer health and safety, environmental law and the digital economy (Bradford, 2020, pp. 99–231). Her analysis includes the development of the GDPR with the extraterritorial effect that is relevant in the context of this article (Bradford, 2020, pp. 131–169). While all five factors are relevant for the establishment of the GDPR as a global standard, the extraterritorial effect is mainly created by a combination of market size and the non-mobile 'data subjects' that represent the inelastic targets in the context of Bradford's theory.

For the purposes of this article, we consider the 'Brussels Effect' a power-based approach, since it combines elements of political and economic capability to determine societal and normative developments in a particular area. The theory emphasises economic scale and political influence, which are more important than Euro-

pean values as such. On a philosophical level, the five factors of the Brussels Effect and much of the EU efforts to spread GDPR norms follow the principles of the framework developed by Emanuel Kant for the establishment of universal peace. Specifically, the second part of the definitive articles that refer to a federal union of sovereign republican states joined by common interests in trade rather than in global civil rights (*Weltbürgerrecht*) indicate the means through which joint norms should be established—a balance of economic interests rather than a joint belief in value (Kant, 1796). We put this power-based approach in contrast to value-based strategies that emerge from human rights law, for instance. Kant has been criticised by Cosmopolitan scholars, amongst others by Jürgen Habermas, for failing to transcend power politics and for being unable to believe in any moral motivation to create and maintain a federation of free states (Habermas, 2000, p. 171). After all, Kant's view of the nature of man is still one that is determined by greed and violence, albeit one that can be compelled by reason (Zwitter, 2015).

To define value-based strategies, it is necessary to consider the 'value' concept. In his seminal work 'Being and Nothingness' (*L'être et le néant*) first published in 1943, French philosopher Jean-Paul Sartre suggests that a value is an entity that exists in the human mind as what it currently is (*Dasein*), and as what it lacks (*manqué*) (Sartre, 2020, pp. 136–162). He uses the parable of the moon for illustration. Over time, it will appear as a crescent moon and 'grow' until it appears as a full disc. Regardless of its present form or colour humans all over the earth refer to this ever-changing entity as one and the same. This common reference object is also one that enables a discourse amongst global citizens. This discourse allows one to transcend the provincial limits of particular forms of our lives and specific ethical norms onto a level where a biggest common denominator can be universally agreed upon. The important difference between norms established through discourse rather than through power is the free consent of all parties and their belief in that norm. A value-based strategy, founded on the free consent through belief of consenting parties, we argue, might be a stronger foundation for realising common norms and for establishing lasting relationships between all parties of the agreement.

Now moving from philosophical considerations to the perspective of European integration, regional institutions such as the Council of Europe and the EU were historically established to 'achieve greater unity between the States of Europe through respect for the shared values of pluralist democracy, the rule of law and human rights' (Polakiewicz, 2021, p. 2). These three overarching categories of values can also be identified in Article 2 of the Treaty on the European Union, which

contains an overview of the values of the EU. When it comes to human rights including privacy, the European Convention on Human Rights (ECHR) has become the central legal reference framework in Europe since the Second World War. The ECHR is usually described as a 'living instrument' since the interpretation of the rights (values) it enshrines changes over time (Theil, 2017, pp. 589–590). It is also essential for the protection of fundamental rights in the EU, according to Article 6 paragraph 2 and 3 of the Treaty on the Functioning of the European Union. Therefore, human rights treaties such as the ECHR and the later developed and corresponding (see Article 53) Charter of Fundamental Rights of the EU (CFEU) enshrine ever-changing values that are observed and interpreted on a case-by-case basis by institutions, such as the Court of Justice of the European Union in Luxembourg (CJEU). From the perspective of EU law, regulatory frameworks, such as the GDPR, need to mirror the human rights (or values) enshrined in the ECHR and CFEU (e.g. GDPR recitals 1, 2, 4, 104).

Whereas power-based approaches focus on elements of political and economic capability to determine societal developments, value-based strategies, such as the ECHR and CFEU, emphasise human dignity, which is considered as the root of modern human rights law (Petersen, 2020). This common norm established as universally valid through discourse provides a stronger and longer-lasting foundation than a power-based approach which focuses on the means (of power capabilities) to achieve norm universality.

We argue that power-based approaches that result in extraterritorial effect do not primarily address the fundamental values at stake. At the same time, this approach to extraterritorial application of norms disrespects the sovereignty and rights of actors that are subject to it (Kamminga, 2020). Certainly, as in the case of the GDPR, some power-based attempts might come with an opportunity to replace less dignified approaches to data protection—such as the protection of personal data as a mere consumer right (Bradford, 2020, pp. 140–141)—with ones that do address it with human dignity at their core (see also Art 1 CFEU). In other words, we acknowledge that the GDPR has had a very positive influence for the strengthening of data protection rights. However, this emphasis on the substance of the right (or the essence of the value) is not a given. In the case of the data protection regulation it is the result of an incremental development of substantive privacy and data protection standards, that took place for more than fifty years. This process started with the first regional data protection law in Hesse in Germany in 1970 and continues since then on many different political and institutional levels (González Fuster, 2014, pp. 213–248; Greenleaf, 2021a, p. 3; Ukrow, 2018, pp.

239–340; van der Sloot, 2014, pp. 307–310).

In conclusion, the outcome of the extraterritorial application of a power-based approach will only enable to govern European values inside data flows for as long as the political actor promoting this position is (1) able to align the 'effect' factors and (2) requires the value-promoting outcome through the regulatory framework. The Brussels Effect and all of its alleged benefits are potentially exchangeable with a 'Beijing Effect' to name just one example. Bradford herself doubts that the Chinese authorities will be able to achieve similar authority, essentially since the relative growth rate of the Chinese economy might be more similar to those in EU countries by the time the institutional capabilities are reached to create the effect. At the same time, the average age in the future Chinese society will be higher and the Brussels Effect will have already influenced standards all over the world, including China itself (Bradford, 2020, pp. 266–270). One of the core differences might be that many norms spread extraterritorially by the EU might already more closely align with universal normative principles and, therefore, might be more readily accepted. Even if the Brussels Effect will not disappear anytime soon, the question still remains whether the value of data protection and privacy can be guaranteed on a high level should the EU and its member states change their political priorities. Before going on to illustrate this conflict between a power-based approach and a value-based strategy in the case studies below, we consider the extraterritorial effect of the GDPR by analysing its legal architecture.

## Section 3. Legal architecture and extraterritorial application

In 2016 the GDPR replaced the Data Protection Directive 95/46 EC of the European Community from 1995 (DPD). Data flows have become increasingly global and relevant for business and governance since the time the DPD was drafted and negotiated. This created the need for more detailed regulation (Kuner, 2010, pp. 246–247) and the requirement to reconsider territorial scope when developing new legal frameworks (de Hert & Czerniawski, 2016, p. 230). The territorial restriction of application has gradually been loosened to address the changed technicalities around the collection, storage, processing and sharing of personal data. In fact, Svantesson rightly flags that the term 'territorial scope' has become misleading on the one hand, while remaining essential for the applicability and enforceability of the GDPR on the other. Hence, territorial scope should not be understood literally. Rather, the concept expresses how GDPR positions itself in the international data sphere, particularly when it comes to the protection of personal data created

through the monitoring and profiling of persons by corporations and public entities (Svantesson, 2019, p. 74). In this section we analyse Article 3 GDPR, which defines the territorial scope of EU data protection law. Additionally, we briefly analyse Article 44-50 GDPR, which regulate transfers of personal data from the EU to third countries and international organisations, with a particular focus on the adequacy decisions as specified in Article 45 GDPR. This article sets forth the procedure and standards that allow the European Commission to assess if non-EU countries and territories have an adequate level of data protection when compared with the GDPR (Kuner, 2019, p. 774).

## 3.1. Article 3 GDPR

In principle, Article 3 and the corresponding recitals 22-25 of GDPR trigger territorial application via two elements: the presence of a relevant establishment of a controller or processor on EU territory, or the targeting or monitoring of data subjects associated with the EU (Van Alsenoy, 2018, pp. 78–79). Article 3 GDPR consists of three paragraphs. [1] In summary, paragraph 1 remains relatively close to the historic nucleus of Article 4 DPD, whereas paragraphs 2 and 3 shift the focus clearly beyond the territory of the EU (Svantesson, 2019, pp. 85–95).

Keeping in mind that the EU is first and foremost an economic community, the point of departure of territorial scope is an establishment on the territory of the EU, which is effectively exercising activities in which personal data is being processed. Both criteria named in Article 3 have been subject to considerable jurisprudence of the CJEU in cases such as *Google Spain (C-131/12)*, *Weltimmo (C-230/14)* and *Verein für Konsumenteninformation (C-191/15)* (Van Alsenoy, 2018, pp. 80–83). This might have sparked the desire of policymakers to expand the territorial scope further once it was clear the DPD would be replaced with GDPR. Hence, Article 3 paragraph 1 GDPR includes not only the 'controller' of the data processing operation, but also the 'processor'. The EDPB attempted to clarify these concepts through non-legally binding guidelines which were adopted on 2 September 2020. There it states that a controller must decide on both purpose and means of the use of personal data, whereas a processor processes data on behalf of the con-

1. *1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

troller, providing technical and organisational support. A processor can be a natural or legal person, as well as a public authority, agency or another body (European Data Protection Board, 2020a, pp. 3–4). Finally, an element of extraterritorial application was added to paragraph 1 by stating that the rules of GDPR apply regardless of whether processing takes place on Union territory or not (Van Alsenoy, 2018, pp. 79–80).

Nevertheless, the most radical shift towards extraterritorial application comes in paragraph 2 of Article 3 GDPR. While the heritage provision in the DPD took the use of certain equipment as reference point, the GDPR focuses on data gathering from European data subjects. As mentioned in recital 14 of the GDPR, the concept of data subject is not limited to natural persons with EU citizenship, permanent residence, or any other legal status (European Data Protection Board, 2018, p. 14). The framework applies to any data subject in the Union if the goods or services are offered to this individual, regardless of where the offer 'comes from', or whether goods or services provided are 'free'. Furthermore, GDPR also applies if data subjects are 'monitored' in their behaviour. While the formulation of the paragraph makes clear that the intention of the drafters of the GDPR was to give it an extraordinarily broad territorial scope, it also creates considerable challenges when trying to interpret and apply it (Svantesson, 2019, p. 95). As noted by Gömann, 'it seems unlikely that the monitoring approach of Article 3(2)(b) GDPR will in practice provide for much more than a declaration of political intent' (Gömann, 2017, p. 588). With such a broad coverage, it is difficult to think of an operation involving personal data carried out by a significant actor in the international data sphere which is not within the territorial scope of GDPR, as most globally available digital services and platforms will at least potentially have to consider that they target EU data subjects.

Moving on to Article 3 paragraph 3 GDPR, the historic background and the corresponding recital suggest that this provision has a specific and limited scope which only relates to the communication of EU member states with their diplomatic missions and consular posts. This also seems to be confirmed by the EDPB in the guidelines on territorial scope adopted on 12 November 2019, where the examples mention a consulate of an EU member state operating in the Caribbean, or a cruise ship serving customers on the high sea (European Data Protection Board, 2018, pp. 22–23). Nevertheless, since the legally binding text of the provision itself is not very specific or limited and seems to be based on questionable interpretations of public international law (Svantesson, 2019, pp. 92–95), it is not helpful in limiting and precisely understanding the territorial scope of GDPR either.

The extensive territorial scope of the GDPR makes it difficult to define its effective—or even intended—reach. Any significantly limiting factor to the scope is missing. Certainly, EU legislators attempted to create a framework for comprehensive protection of the rights of data subjects with an eye towards establishing a level economic playing field for competition in data-driven services across the EU and worldwide (European Data Protection Board, 2018, p. 4). However, this results in a situation where global actors in the digital sphere—such as large digital platforms or manufacturers of consumer electronics which market their products in several regions—have to decide whether GDPR applies in its entirety with all compliance requirements for their operations, or not at all. This conclusion is in line with the power-based approach that we defined in Section 2. Therefore, it is fair to state that with such an extensive territorial scope, GDPR is a polarising factor in the international data sphere, with actors outside the traditional scope of EU regulations having to comply with one of the most demanding data protection regulations globally. While it allows the EU to demand high standards when it comes to the protection of individual rights, it also raises questions on legitimacy, practicality, as well as legal certainty and enforceability.

Briefly addressing the aspects of legitimacy and practicality, de Hert and Czerniawski (2016, p. 240) proposed to establish a 'centre of gravity' test for the application of the GDPR, using factors such as minimum connection of the activity, purpose and enforceability. Similarly, a 'layered approach' can be found in the work of Svantesson. This entails consideration of the harm being caused for individuals by a specific data operation, taking into account how essential the infringed provisions of GDPR are, as well as balancing the cost and effects of enforcement with a final proportionality assessment (Svantesson, 2019, pp. 95–96).

When it comes to legal certainty and enforceability, there have been demands to deliver more guidance on key terms since the drafting of Article 3 GDPR (Van Alsenoy, 2018, p. 97). As we showed throughout this section, the EDPB has attempted to respond to those with Guidelines 07/2020 on the concepts of controller and processor, as well as with guideline 03/2018 on territorial scope. Nevertheless, these guidelines are ultimately not sufficient for two reasons: First, they themselves do not provide the amount of detail required. As guidelines, they need to keep a relatively high level of abstraction, frequently merely clarifying the applicable provisions and recitals within the regulation. However, it is the vague nature and wording of the articles in the GDPR that is the key problem. Secondly, the guidelines are not of legally binding nature. While it is commendable that European data protection authorities try to establish certainty, the authority to shape

EU law is vested with the legislative bodies (European Parliament and European Council), and the authority to interpret it rests with the CJEU according to Article 19 paragraph 1 TEU.

## 3.2. International data transfers and adequacy decisions

To be able to comprehensively analyse the case studies in Section 4 we also have to consider the regime that regulates international data transfers. According to Article 44 GDPR, personal data can only be transferred out of the EU if the principles of the regulation are upheld. Chapter V contains Articles 44-50 GDPR to regulate such transfers and, according to Kuner, establishes a three-tiered structure that puts adequacy decisions at the top, appropriate safeguards in the middle and derogations at the bottom (Kuner, 2019, p. 774). An adequacy decision can be roughly described as a 'data bridge', which has the purpose of facilitating the international flow of data. The main advantage is that it renders other individual agreements creating a legal basis for transfers unnecessary. Examples for such alternatives are standard contractual clauses, binding corporate rules, or individual consent for single instances of data collection and processing. If the EU Commission finds that there is an adequate protection of personal data in another country, this simplifies business activities and other data-driven cooperation.

From a legal perspective, adequacy decisions are implementing acts issued by the European Commission, based on an assessment of the formal level of protection of personal data in another country. In other words, they do not involve the European Council (ministers of member states) or the European Parliament, but the Commission has to consult the EDPB (Greenleaf, 2021b, p. 23; Kuner, 2019, p. 785). As we will further outline in the second case study, the case law of the CJEU has become increasingly influential in outlining the criteria for adequate protection in countries outside the EU. This is especially the case with regard to the '*Schrems I*' (C-362/14) and '*Schrems II*' (C-311/18) judgments dealing with complaints against European Commission adequacy decisions known as 'Safe Harbour' and 'Privacy Shield' in regard to transatlantic data flows with the United States. These heavily influenced interpretation and application of the GDPR and a detailed description of them in the context of extraterritoriality is appropriate (Tzanou, 2020, pp. 100–114). Since there is currently some uncertainty on how the criteria that were developed by the CJEU in these judgments could best be implemented and enforced (e.g. by the Irish Data Protection Authority against Facebook, Busvine & Humphries, 2021), it became unavoidable to start a process of updating alternatives such as standard contractual clauses for international data transfers of private corporations (Boardman, 2020). Additionally, the EDPB adopted guidelines for

international data transfers between public bodies in application of Articles 46 paragraph 2a and 46 paragraph 3b GDPR on 15 December 2020 (European Data Protection Board, 2020b). For the purposes of this article, we will not discuss them in further detail since the effects around the declaration of adequacy are most relevant.

We acknowledge that from a legal perspective an adequacy assessment only covers whether personal data can leave the EU, which raises the question whether adequacy decisions actually have extraterritorial effect. However, we argue that such a mono-disciplinary analysis neglects their political and economic character. Taking an interdisciplinary perspective, adequacy decisions do have extraterritorial effect since they provide an incentive—along the lines of the power-based approach—to update or revise national data protection laws. This has most recently been demonstrated in the cases of Japan and South Korea, which both have updated and aligned their national laws with the GDPR in attempts to have privileged access to the EU single market (Greenleaf, 2021b, p. 23). The adequacy decision for Japan was adopted on 23 January 2019 and is the first under the GDPR framework (Commission Implementing Decision (EU) 2019/419), while the talks with South Korea were successfully concluded on 30 March 2021 (European Commission, 2021c). Both adequacy assessments are part of a larger political package that mainly consists of a Free Trade Agreement. Fahey and Mancini argue that the Japanese adequacy decision was a 'side-product of the EU-Japan Economic Partnership Agreement […]: despite the EU's initial goal of excluding data from the trade negotiations, Japan insisted on data dialogues and the EU eventually accommodated the demands' (Fahey & Mancini, 2020, p. 99). Certainly, rigid fundamental rights-inspired interpretations of data protection may create possibly unwelcome burdens for certain political branches of the EU itself (Ryngaert & Taylor, 2020, p. 7). However, this demand for flexibility in political negotiations with international partners raises doubts as to whether the EU is able to consistently apply European values such as human rights when scrutinising adequacy. At least the question of standardisation of adequacy procedures emerges, which could help to guide the Commission in producing more consistent adequacy assessments. This necessity for more procedural standardisation is not only visible in the context of the second case study in section 4.2 that covers the persistent uncertainty in transatlantic data flows as the United States effectively refuses to directly safeguard the rights of EU data subjects through changes of their laws and institutions. As Drechsler (2020) outlines, the difficulty to assess adequacy on the basis of values—such as the EU human rights catalogue—also exists when considering the larger context of the EU data protection package that includes the EU Law Enforcement Directive

2016/680.

# Section 4. Case studies

We will now consider whether extraterritorial application of the GDPR promotes European values or power in the context of two case studies. We propose that discussion of the developments around the RTBF is particularly relevant since this individual right has been hailed as one of the central mechanisms that enables individuals to control personal data, although the vague territorial scope was a challenge from inception (Ausloos, 2020, pp. 98–104). The question of territorial scope and platform governance has also come up in the prominent *Glawischnig-Piesczek* case (C-18/18) that was decided by the CJEU on 3 October 2019. This case originated in 2016, when the former leader of the Austrian Green Party Eva Glawischnig-Piesczek started a procedure against another Facebook user that insulted her on the platform. The user posted inappropriate comments that criticised the political position of Glawischnig and the Green Party on migration issues (Kuczerawy & Rauchegger, 2020, pp. 1496–1498). Questions around the responsibility and role of Facebook in removing this inappropriate content from the platform led to the CJEU case, with the result that identical and similar comments needed to be deleted for all users globally. This finding was finally implemented by the Austrian courts with a decision of the high court of last instance from 15 September 2020 (Oberster Gerichtshof, 2020b, 2020a). While some aspects of this case show similarities to the discussion around the territorial scope of a RTBF, the case is not relevant in the context of this article since it does not relate to the GDPR or data protection. The relevant legal frameworks in the *Glawischnig-Piesczek* case include the EU eCommerce Directive (especially Article 15 paragraph 1 of Directive 2000/31/EC), the EU Directive on Copyright in the Digital Single Market 2019/790, as well as, potentially, the proposed EU Terrorist Content Regulation and the proposed EU Digital Services Act (Kuczerawy & Rauchegger, 2020, pp. 1495–1496). In order to keep the analysis focused and remain in the GDPR framework we have therefore decided not to further elaborate on this case. Finally and additionally to what has been outlined in section 3.2., discussion of the adequacy regime is particularly relevant since it allows one to outline the intended territorial scope of GDPR, as well as how the EU positions itself in data protection related matters against other influential actors, such as the United States.

## 4.1. Extraterritoriality and the 'right to be forgotten'

One of the key promises of GDPR was the effective and comprehensive protection of individual rights in the digital sphere. This relates not only to traditional as-

pects such as transparency, fairness and notification (van der Sloot, 2014, pp. 310–314), but also to more novel and challenging scenarios such as the deletion of personal data from the entirety of the internet. This RTBF for the digital age was first envisaged by Viktor Mayer-Schönberger in 2007 (Mayer-Schönberger, 2011, p. ix), and subsequently integrated in the first proposal for GDPR by the European Commission as an extension of a 'right to erasure' at the beginning of 2012. Since that time much has been written about the desirability of a RTBF, as well as the final Article 17 GDPR (Ausloos, 2020).

Well before GDPR was finished, the discussion on how to operationalise a RTBF started to crystallise around the responsibilities of search engine operators (SEOs) on how to structure links in search results. This affected Google in particular due to its market dominance in the EU. In the seminal *Google Spain* judgment of 13 May 2014 (C-131/12) the interpretation of the concepts of processor and controller by the CJEU was central (Van Alsenoy, 2018, pp. 81–83), as well as the balancing act between privacy and freedom of expression (Gstrein, 2017, pp. 9–10). While territorial scope has also been an issue in *Google Spain*, this aspect took the spotlight more recently in the case of *Google vs CNIL*, which was decided in Luxembourg on 24 September 2019 C-507/17 (see Samonte, 2020, pp. 841–844). In principle, there are three options for territorial scope; delisting can be limited to EU territory, enforced as a universal norm which has to be applied globally on all versions of a search engine and for all users, or implemented 'glocally' (Padova, 2019, pp. 21–29). This last approach does not mean that a service has to have servers physically on EU territory, but that measures such as geolocation of the user based on the monitoring of Internet Protocol (IP-)Addresses or GPS-location could be used to determine the physical position of the user and serve/hide search results accordingly. This could potentially result in the necessity to reduce the privacy of users when using a search engine, while being able to uphold local or cultural expectations of one region (e.g. not showing swastikas in search results in countries where this is forbidden for political and historical reasons). The extent to which this affects other regions varies with the detailed technical and organisational implementation, which is largely left to SEOs (Powles & Chaparro, 2015).

Briefly summarising the complex procedure, the French data protection authority (*Commission Nationale de l'Informatique et des Libertés* or CNIL) was not satisfied with the implementation of the delisting of links in search results adopted by Google in the aftermath of the Google Spain judgment from 2014. The argument of CNIL essentially boils down to the universality of an individual right enshrined in GDPR. According to the authority, such a right can only truly manifest itself if

enforced on all versions of a search engine, even those operated outside the EU. If links to search results are not removed on all versions, an individual travelling back and forth between France and the United States who is seeking personal information about a business partner for instance, could access controversial information easily when in the United States, while this is more difficult in France. Such extraterritorial application of the GDPR was heavily contested (Keller, 2018) and Google itself tried to limit the territorial reach of delisting to the European versions of its search engine. Additionally, it adopted some technical measures to tie search results to regions, such as the analysis of user IP-addresses. After fighting over the implementation of delisting in French courts, the issue went back to the CJEU (Gstrein, 2020, pp. 130–133).

In contrast to the ground-breaking judgment from 2014, the 2019 decision of the CJEU took place in greatly changed circumstances. The GDPR was finalised and in force, which brought considerable requirements for corporations and public institutions to comprehensively overhaul their privacy policies and data practices (Linden et al., 2020, p. 62). Concordantly, even the European Commission acknowledges in its review of GDPR from June 2020 that the enforcement of the regulation is a challenge for data protection authorities (European Commission, 2020a, p. 5). Given the EU-internal pressure not to overburden institutions of member states by making them guardians of data subject rights all over the globe, plus the external pressure not to interfere too strongly in international data flows and business, the restraint in Google vs CNIL makes sense politically.

However, courts like the CJEU are supposed to interpret the law, and not to make political decisions. Nevertheless, the judges essentially avoided defining further the substantive nature and territorial scope of delisting in *Google vs CNIL*. While the Grand Chamber around president Lenaerts seemed to favour a 'glocal' approach, it did not provide any firm interpretations and left a space of discretion for the authorities of member states (see paragraphs 64-72 of C-507/17). This vacuum of guidance on the European level was quickly seized by the German Federal Constitutional Court, which published two judgments on the RTBF shortly after the CJEU, on 6 November 2019. The German judges did not only further define the substantive nature in the context of the German legal order, they also sent an implicit message to the rest of the EU: digital rights such as a RTBF ought to be shaped through dialogue between the EU and its member states, and not be the product of a hierarchy with Brussels/Luxembourg at the top (Gstrein, 2020, pp. 136–139).

One can interpret these events from an intra EU perspective, where they demon-

strate that progressive and consistent leadership on data flow-related rules is essential for European institutions to be able to shape the dynamic of events, as well as preserving European unity. At the same time, however, such focus on internal power struggles misses the point that the RTBF is not a European concept. While the EU and the jurisprudence of the CJEU has certainly been instrumental in making the RTBF a broadly known concept, it exists in many countries around the world and similar protections are enshrined in the majority of data protection frameworks of G20 member states (Erdos & Garstka, 2021, pp. 308–310; Gstrein, 2020, pp. 141–143). Hence, 'the robust realization of a RTBF online will certainly require transnational consensus-building and coordination extending well beyond the EU Member States' (Erdos & Garstka, 2021, p. 296). In the context of this article, we interpret this finding as a call for the development of a value-driven strategy to achieve more international consensus on the substantive dimension and territorial application of the right.

## 4.2. Inadequacy of data bridges without pillars

As outlined in Section 3.2., one of the central tools for positioning European digital space in relation to other regions is adequacy decisions, which are regulated in Article 45 GDPR. Currently, the EU Commission has fourteen adequacy decisions in place (e.g. for Switzerland, Israel, Japan and two for the United Kingdom), with the likely positive decision for South Korea imminent at the time of writing (European Commission, 2021a). However, the most discussed and contested decisions so far are those relating to the United States. Two adequacy decisions by the Commission have already been declared void by the CJEU, most recently bringing an end to the 'EU-US Privacy Shield' with the judgment in *Schrems II* from 16 July 2020 (C-311/18; (Tracol, 2020, p. 1).

While the end of Privacy Shield was not surprising for many experts, it created considerable uncertainty for more than 5,300 companies that relied on it as a legal basis for their data transfers (Propp & Swire, 2020). According to the Annual Governance Report 2019 of the International Association for Privacy Professionals (IAPP), the Privacy Shield was used by 60 percent of the respondents and only surpassed by standard contractual clauses used by 88 percent (IAPP, 2019). However, the discussion as to which extent *Schrems II* also invalidates the use of alternatives to an adequacy decision is still ongoing among legal experts, and the onus to prove compliance with legal requirements is on businesses and public institutions transferring data between the regions (Irion, 2020; Propp & Swire, 2020). Ad hoc, a combination of standard contractual clauses and additional technical and organisational measures (e.g. use of strong encryption) seem like a viable strategy (Chris-

takis, 2021b; Tracol, 2020, pp. 9–11; European Data Protection Board & European Data Protection Supervisor, 2021).

*Schrems II* has many aspects worth analysing, but in the context of this article we focus on the consequences of the judgment for the territorial scope of GDPR. As the CJEU reiterates at paragraph 52 of the judgment, the territorial aspect is essential since, according to the complaint of Austrian digital rights activist Max Schrems, the United States 'did not ensure adequate protection of the personal data held in [their] territory against the surveillance activities in which the public authorities were engaged.' The investigation of such a claim puts the CJEU in a delicate position for two reasons.

First, any scrutiny of the Privacy Shield entails the necessity of an assessment of the protection of personal data of EU data subjects when it comes to surveillance by US authorities. Whereas the CJEU refrained in 2015 from analysing and discussing the details of US law (e.g. Section 702 of the Foreign Intelligence Surveillance Act or Executive Order 12333) in *Schrems I* and instead focused on the characteristics of a valid adequacy decision, *Schrems II* contains detailed findings on the necessity and proportionality of some US surveillance programmes (see C-311/18 paragraphs 165, 166, 178 to 184, 191 and 192; (Tracol, 2020, p. 7; Tzanou, 2020, pp. 109–114). Hence, it may not be entirely surprising that the judgment has also been described as a 'mix of judicial imperialism and Eurocentric hypocrisy' (Baker, 2020). Secondly, the CJEU lacks the competency to carry out a similar assessment on the situation regarding governmental surveillance for a member state of the EU (Christakis, 2021a). While the EU Fundamental Rights Agency has highlighted in a research report that intelligence laws in European states remain complex, with potential to improve oversight as well as effective individual remedies (European Union Agency for Fundamental Rights, 2018, pp. 9–10), Article 4(2) of the Treaty on the EU excludes national security from the competences of EU institutions.

The CJEU certainly tries to leverage the power of European data protection law through the *Schrems II* judgment to create higher protection standards for EU data subjects. However, remembering the fierce defence of the autonomy of EU law in the CJEU opinion on the accession to the European Convention on Human Rights in 2014 (Halberstam, 2016), it seems unlikely that the Grand Chamber of the CJEU is not following a carefully considered strategy. The question is to which degree this is a value- or power-based strategy, and we will return to this aspect and alternatives in the discussion and conclusion.

Regardless of the answer, the current levels of legal and political uncertainty make it increasingly attractive to keep personal data in the EU (Tracol, 2020, p. 11). While the European Commission has announced to start work on a third iteration of the EU-US data bridge (European Commission, 2020b), it is also obvious that the pillars of this bridge will only stand if political concessions are made on the American side with regards to the establishment of effective and accessible individual remedies for GDPR data subjects. In other words, the judgments in *Schrems I* and *Schrems II* gradually build pressure on the United States to change their own regulatory framework and institutions in a way that could be similar to Japan and South Korea. At the same time the question emerges if the European Commission might be more inclined to grant adequacy if the question of data protection becomes part of a larger political package that might involve economic benefits. Potentially, the perspective of adequacy could result in an upgrade of the US privacy regime, which could embrace some or all of the basic principles of the GDPR. Alternatively, some US-based commentators are optimistic that the requirements of *Schrems II* can be met with relatively little adjustment and reconfiguration of existing judicial and administrative institutions (Propp & Swire, 2020). Whichever route the European Commission and all actors involved choose, ultimately any new framework will most likely have to stand another test of the CJEU.

## Section 5. Discussion

As Van Alsenoy puts it, '[e]xtraterritoriality and data protection make for a controversial mix. Different attitudes towards privacy, coupled with a lack of global consensus on jurisdictional boundaries, fuel an intense debate among those advocating jurisdictional restraint and those emphasizing the need to ensure effective protection' (Van Alsenoy, 2018, p. 77). As has been shown in section 3.1., Article 3 GDPR is a vague provision that creates legal and political uncertainty. The current design of the legal framework results in friction when it comes to the precise scope of individual rights and makes it challenging to guarantee consistency and stability in international data flows. Additionally, adequacy decisions and the GDPR regime regulating international data flows might be strongly influenced by economic policy, which comes with the danger that the underpinning values of GDPR are consistently respected and protected by the EU. For instance, Greenleaf criticised the lack of consistency and level of rights protection of the draft agreement for the Japanese adequacy decision, questioning whether there is a discounted version of adequacy under certain circumstances (Greenleaf, 2018b). While one might welcome that it was possible for the two systems to open up to each other (Miyashita, 2020, p. 13), the question arises which kind of institutional safeguards

are in place to guarantee consistent application of high data protection standards. The procedure to assess adequacy seems to lack standardisation as shown by a comparison with South Korea (Greenleaf, 2018a). In order to avoid the negative side effects of a power-based approach the EU system currently relies on members of civil society such as Max Schrems to check the decisions, which leads to lengthy legal procedures with uncertain outcomes.

At the same time, as the existence and increasing number of jurisdictions outside the EU and the United States with a RTBF demonstrates, there might be more potential for international harmonisation and consensus on the rights of data subjects than expected. While there seems to be little desire to have a power-based European leadership on data protection, the principles and rights enshrined in the GDPR inspire legislators across the world to adopt similar provisions. Even some US states such as California have recently begun to update their regulatory framework, which also takes into account some GDPR features and principles (Rothstein & Tovino, 2019, p. 5; Chander et al., 2021).

## 5.1. Alternative multilateral frameworks

Treaties that qualify individual rights as the object of fulfilment are special agreements in public international law. In their traditional form, they create a triangular relationship between participating states and their citizens. The duty-bearer remains the state, which is obliged to respect and protect the stipulated rights of the individuals it is responsible for (Zwitter & Lamont, 2014, pp. 363–365). Hence, such treaties ultimately create substantively harmonised national legal frameworks, which hinge on reciprocity and mutual respect as methods of enforcement on an international level. This guarantees the sovereignty of states, yet makes it challenging to enforce individual rights if remedies are not effective on a national level, or if the cause of infringement lies beyond the territory of the state. While there is an emerging realisation that privacy should be treated as a universal human right and guaranteed across and beyond territorial borders, the manifestation of this insight still requires time (Irion, 2020).

When searching for existing frameworks capable of the establishment and harmonisation of high data protection standards at the global level the only existing and legally binding international treaty is the Council of Europe Convention 108 for the protection of individuals regarding automatic processing of personal data (Cannataci, 2018, pp. 21-22). The Convention has been discussed as a global standard in contrast to portraying the GDPR as a gold standard (Mantelero, 2020, pp. 1–3). The recently overhauled 'Convention 108+' shares many principles, individual

rights and features with the GDPR but allows each signing state to adopt corresponding national laws which further define the principles. This modernised framework was opened for signature in Strasbourg on 25 June 2018 (Ukrow, 2018, p. 240). States which are not members of the Council of Europe can also join it. As of September 2021, 30 states have signed Convention 108+, of which 13 have already ratified it (Council of Europe, 2021). Hence, a potentially more sustainable and multilateral strategy than power-based extraterritorial application to promote European values inside international data flows might be to emphasise value-driven harmonisation more strongly, focusing on an open mind that seeks to identify common denominators where they exist. However, the relationship between the EU and the Council of Europe is complex. Polakiewicz recently highlighted again the lack of consistency, transparency and clarity when it comes to voting rights and speaking rights of the EU, as well as financial arrangements (Polakiewicz, 2021, p. 18).

## 5.2. A future without allies?

While the cases presented in this article focus almost exclusively on the current relationship between the EU and the United States, it also needs to be added that the data flows to and from other countries and regions increasingly face similar challenges. For instance, during the work on this article adequacy decisions have been adopted with regards to the United Kingdom, addressing the consequences of Brexit. This process was launched by the European Commission on 19 February 2021 and the EDPB presented opinions relating to a GDPR and EU Law Enforcement Directive adequacy decision on 16 April 2021 (European Commission, 2021b; European Data Protection Board, 2021). On 28 June 2021 the Commission announced the adequacy decisions which are based on the GDPR and the Law Enforcement Directive. It remains to be seen how fruitful the relationship between the two parties can become over the long term, especially in areas where the United Kingdom might seek to deviate in data protection standards governing the development of data-driven services, or opt for extensive data use for surveillance (European Commission, 2021d; Korff, 2021). It does seem possible that the Council of Europe will gain a more important role in the relationship between EU member states and the United Kingdom after Brexit, especially when it comes to safeguarding the right to privacy of individuals which is also protected by the ECHR framework.

Additionally, the intense economic cooperation of many EU countries with the People's Republic of China leads to questions around the treatment of data flows and the standards used when it comes to personal data. In June 2020, reports emerged

of a court case in the German town of Düsseldorf in which a former manager of Huawei was not given access to personal data stored by the company in China that might have been relevant to support his position in the case. The labour court found that Huawei needs to pay €5.000 in immaterial compensation for the damage suffered by the former employee, which was based on Article 5(2) in connection with Article 82 GDPR. However, it remains to be seen whether this decision of first instance (ArbG Düsseldorf v. 5.3.2020 - 9 Ca 6557/18) will be confirmed as there was an appeal by Huawei (Wybitul, 2020).

The question of how to guarantee effective enforcement of high data protection standards certainly remains essential. As the CJEU judgments on the EU-US adequacy decisions and the surrounding political and societal developments have demonstrated over the last years, the current approach to establish European values inside data flows exceeds the capabilities of GDPR on the one hand and reduces its implementation increasingly to a battlefield on the other. This does not only reveal that the promises on the universality of the rights of a data subject enshrined in the regulation are not realistic. Additionally, such a limited approach also fails to address the overarching issue, which is that the protection of personal data under current circumstances is systematically threatened. While it should be welcomed that GDPR re-emphasised the importance of data protection and that EU data protection authorities now have more competences and powers to address an urgent problem, it is also clear that the fulfilment of the task is overwhelming. One should not forget that '[t]he need to ensure trust and the demand for the protection of personal data are certainly not limited to the EU. Individuals around the world increasingly value the privacy and security of their data' (European Commission, 2020a, p. 2).

It is also noteworthy that those public institutions which try to provide certainty are the national data protection authorities in the form of the EDPB, as well as the CJEU. However, as has been shown throughout this article, the powers transferred to them by constitutional law and the EU treaties limit their possibilities. The function of the court is to interpret European law and the core task of data protection authorities is to independently monitor the situation and enforce the legal order when necessary. This requires that the legal frameworks in place are designed in a way that is consistent and serves a clear purpose which is based on fundamental constitutional provisions and values such as human rights. In that regard, the extraterritorial effect of GDPR and the associated enforcement can only overwhelm the authorities and come with undesired side effects. This brings us to the last point, which is the lack of political leadership. Specifically, more attention

needs to be paid to craft clear legal provisions that establish certainty, even if this means that an EU-internal compromise is harder to achieve throughout legislative negotiations. It is clear that extraterritorial application and unilateral standard-setting face severe limitations with the potential to harm the original cause in the long-term. At the same time, while there are a limited number of options available to establish reliable multilateral governance frameworks for the protection of personal data, there is still the potential for more cooperation that must be explored and acted upon.

## 5.3. Limitations of the value versus power dichotomy

Throughout this article we have treated power-based and value-based approaches as mutually exclusive. We have done this in order to highlight that the GDPR should not uncritically be considered as the only positive force for the establishment of high and universal global privacy and data protection standards. We have outlined our thinking in the preceding sections and flagged areas and cases where we believe that caution is warranted when applying and enforcing the GDPR. As we have shown in the introduction and throughout by referring to the work of Greenleaf and others, consensus around the substantive core of the regulation is increasingly building. At the same time, European institutions are overburdened in globally enforcing the regulation and political tensions are building, which threatens consistency and the credibility of the EU.

Nevertheless, treating power and value-based approaches as mutually exclusive falls short of the complex reality of internet governance. In order to shape digital spaces, states are not able to rely on traditional patterns of territorial sovereignty and depend more strongly on private actors and their powerful platforms. It has been argued that the GDPR is one of the most powerful symbols of a 'digital constitutionalism' of the EU through which it aims to protect essential values such as human rights and democracy even beyond the borders of the member states. However, the question remains whether in a next phase this leads to what De Gregorio describes as 'privacy universalism'—including a lack of legal certainty and imperial tendencies—or 'digital humanism' with human dignity at the core (De Gregorio, 2021, pp. 63–70). We would very much opt for the latter, which—in the European context—has been achieved after the Second World War through the establishment of multi-level governance mechanisms with international, supranational and national layers that mutually reinforce efforts to promote values and check power. Institutions such as the ECtHR or the CJEU were able to control institutions and authorities of the other layers in cases where values were threatened. In a long-term perspective since the Second World War this system has worked reasonably

well for a Europe that goes beyond the EU. Ideally, a similar dynamic could also be established gradually on a global level. In our view, the mutually reinforcing process that led to the establishment of the substantive principles of the GDPR with influences from the international, supranational and national layers is as important as the legislative end product.

Certainly, the international community has so far achieved too little when it comes to the development of detailed international standards for privacy protection. We are not ignoring the fact that the proceedings in multilateral fora can be dominated by power-based approaches failing to deliver the desired results. Organisations such as the United Nations can be heavily influenced by single actors who leverage their power and influence to undermine sincere discussions about values and principles. Nevertheless, also the EU and its member states will only be able to sustainably pursue a value-based strategy if their own political interests are balanced and checked by institutions and actors from all different governance layers. Finally, as we have outlined above, a value-based strategy based on the free consent and belief of the involved parties might be a stronger foundation for realising common norms and for establishing lasting relationships. A recent report on internet and jurisdiction in Latin America and the Caribbean formulated it in the following way: Is there room for cross-fertilization, or is this mere replication? (Economic Commission for Latin America and the Caribbean (ECLAC) et al., 2020, p. 15). In order to deliver answers to this question political actors within and beyond Europe would have to decide on and engage in international fora where constructive exchange is possible.

## Section 6. Conclusion

This article has explored whether extraterritorial application of the GDPR is promoting European values inside data flows. While the regulation has received considerable attention internationally and has had a positive influence on the level of data protection globally, we argued that the significant extent of extraterritorial application in the GDPR is not a viable long-term strategy to guarantee respect, protection and promotion of European values. Rather than keeping the function of GDPR limited to the essential issue—the protection of personal data—it transforms the regulation into a battlefield for legal, economic and political conflicts.

As we have discussed in the analysis of the legal architecture of Article 3 GDPR, the provision contains vague language and is difficult to interpret and implement. It contains passages that read like political statements (Gömann, 2017, p. 588), which requires additional interpretation from the EDPB, the CJEU and academics.

However, any one of these parties lacks the democratic legitimacy to make such far reaching decisions, which are essential for the applicability of the regulation. This becomes particularly apparent in the discussion about the territorial scope of the RTBF. Additionally, the failed attempts to establish an adequate framework for data transfers between the EU and the United States demonstrates that there is still a considerable gap between the normative aspirations in the regulation and the political reality. It is not impossible to bridge this gap and the consistency of the CJEU in upholding high standards for data protection as well as increased demands of civil society to protect personal data make it unlikely that convenient political trade-offs will create lasting solutions.

Ultimately, the question remains whether the next evaluation report of the GDPR by the European Commission—which is planned for 2024 (European Commission, 2020a, p. 14)—will reflect on a governance strategy of the digital sphere that is driven by the protection of power or the promotion of values. The creation of the latter is not only dependent on upholding and further clarifying existing frameworks but also on the creation of safe venues for substantive dialogue to establish broader international consensus, as well as the commitment to high and effective protection of human rights, which are guaranteed internationally regardless of individual privilege or status.

**ACKNOWLEDGMENTS**

We are grateful to Liz Harvey for reviewing this manuscript.

## References

Ausloos, J. (2020). *The Right to Erasure in EU Data Protection Law* (1st ed.). Oxford University Press. https://doi.org/10.1093/oso/9780198847977.001.0001

Baker, S. A. (2020, July 21). How Can the U.S. Respond to Schrems II? Lawfare [Blog post]. *Lawfare*. https://www.lawfareblog.com/how-can-us-respond-schrems-ii

Boardman, R. (2020). European Commission publishes proposed replacement SCCs. In *International Association of Privacy Professionals*. https://iapp.org/news/a/european-commission-publishes-proposed-replacement-sccs/

Bradford, A. (2012). The Brussels effect. *Northwestern University Law Review*, *107*(1), 1–68. https://scholarlycommons.law.northwestern.edu/nulr/vol107/iss1/1/

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University

Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Busvine, D., & Humphries, C. (2021). *Facebook faces prospect of 'devastating' data transfer ban after Irish ruling*. https://www.reuters.com/business/legal/facebook-data-transfer-ruling-irish-court-due-friday-2021-05-14/

Cannataci, J. (2018). *Big Data and Open Data—Annual Report to the 73rd session of the General Assembly* [Annual report]. United Nations Special Rapporteur on the right to privacy. https://undocs.org/A/73/438

Chander, A., Kaminski, M., & McGeveran, W. (2021). Catalyzing Privacy Law. *Minnesota Law Review*, *105*, 1732–1802. https://minnesotalawreview.org/wp-content/uploads/2021/04/3-CKM_MLR.pdf

Christakis, T. (2021a). *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 1)*. European Law Blog. https://europeanlawblog.eu/2021/04/12/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part1/

Christakis, T. (2021b). *Squaring the Circle? International Surveillance, Underwater Cables and EU-US Adequacy Negotiations (Part 2)*. European Law Blog. https://europeanlawblog.eu/2021/04/13/squaring-the-circle-international-surveillance-underwater-cables-and-eu-us-adequacy-negotiations-part2/

Commission, E. (2021a). *Data protection: Draft UK adequacy decision [Text*. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661

Commission, E. (2021b). Joint Statement by Commissioner Reynders and Yoon Jong In. In *Chairperson of the Personal Information Protection Commission of the Republic of Korea [Text]*. *European Commission—European Commission*.

Commission, E. (2021c). *Commission adopts adequacy decisions for the UK*.

Council of Europe. (n.d.). *Chart of signatures and ratifications of Treaty 223*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

De Gregorio, G. (2021). The rise of digital constitutionalism in the European Union. *International Journal of Constitutional Law*, *19*(1), 41–70. https://doi.org/10.1093/icon/moab001

Drechsler, L. (2020). Comparing LED and GDPR Adequacy: One Standard Two Systems. *Global Privacy Law Review*, *1*(2), 93–103.

Economic Commission Latin America and the Caribbean (ECLAC), Internet & Jurisdiction Policy Network (I&JPN), & Souza, C. A. (2020). *Internet & Jurisdiction and ECLAC Regional Status Report 2020* (Report LC/TS.2020/141). https://www.cepal.org/en/publications/46421-internet-jurisdiction-and-eclac-regional-status-report-2020

Erdos, D., & Garstka, K. (2021). The 'right to be forgotten' online within G20 statutory data protection frameworks. *International Data Privacy Law*, *10*(4), 294–313. https://doi.org/10.1093/idpl/ipaa012

European Commission. (2020a). *Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition—Two years of application of the General Data Protection Regulation*. European Commission.

European Commission. (2020b, July 16). *Opening remarks by VP Jourová and Cmner Reynders*. Press Corner. https://ec.europa.eu/commission/presscorner/detail/en/statement_20_1366

European Commission. (2021). *Adequacy decisions. How the EU determines if a non-EU country has an adequate level of data protection*. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

European Data Protection Board. (2018). *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)—Version adopted after public consultation*. European Data Protection Board. https://edpb.europa.eu/our-work-tools/our-documents/riktlinjer/guidelines-32018-territorial-scope-gdpr-article-3-version_en

European Data Protection Board. (2020a). *Guidelines 07/2020 On the concepts of controller and processor in the GDPR*. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en

European Data Protection Board. (2020b). *Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en

European Data Protection Board. (2021, April 16). *EDPB Opinions on draft UK adequacy decisions* [News release]. News. https://edpb.europa.eu/news/news/2021/edpb-opinions-draft-uk-adequacy-decisions_en

European Data Protection Board & European Data Protection Supervisor. (2021). *Joint Opinion 2/2021 on the European Commission's Implementing Decision on standard contractual clauses for the transfer of personal data to third countries*. https://edpb.europa.eu/sites/default/files/files/file1/edpb_edps_jointopinion_202102_art46sccs_en.pdf

European Union Agency for Fundamental Rights. (2018). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union. Volume II: summary.* Publications Office of the European Union. https://data.europa.eu/doi/10.2811/84431

Fahey, E., & Mancini, I. (2020). The EU as an intentional or accidental convergence actor? Learning from the EU-Japan data adequacy negotiations. *International Trade Law and Regulation*, *26*(2), 99–111.

Gömann, M. (2017). The new territorial scope of EU data protection law: Deconstructing a revolutionary achievement. *Common Market Law Review*, *54*(2), 567–590.

González Fuster, G. (2014). The Right to the Protection of Personal Data and EU Law. In G. González Fuster (Ed.), *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (pp. 213–252). Springer International Publishing. https://doi.org/10.1007/978-3-319-05023-2_7

Greenleaf, G. (2018a). Japan and Korea: Different Paths to EU Adequacy. *Privacy Laws & Business International Report*, *156*, 9–11.

Greenleaf, G. (2018b). Japan: EU adequacy discounted. *Privacy Laws & Business International Report*, *155*, 8–10.

Greenleaf, G. (2021a). Global data privacy laws 2021: Despite COVID delays, 145 laws show GDPR dominance. *Privacy Laws & Business International Report*, *169*(1), 3–5.

Greenleaf, G. (2021b). Global data privacy laws 2021: Uncertain paths for international standards. *Privacy Laws & Business International Report*, *169*(1), 23–27.

Gstrein, O. J. (2017). The Right to Be Forgotten in the General Data Protection Regulation and the aftermath of the "Google Spain" judgment (C-131/12). *PinG Privacy in Germany*, *1*. https://doi.org/1

0.37307/j.2196-9817.2017.01.06

Gstrein, O. J. (2020). Right to be forgotten: European data imperialism, national privilege, or universal human right? *Review of European Administrative Law*, *13*(1), 125–152. https://doi.org/10.7590/187479820X15881424928426

Habermas, J. (2000). Kant's Idea of Perpetual Peace: A Two Hundred Years Historical Remove. In C. Cronin & P. Greiff (Eds.), *The Inclusion of the Other: Studies in Political Theory* (pp. 165–201). MIT Press.

Halberstam, D. (2016). Opinion 2/13 of the Court (C.J.E.U). *International Legal Materials*, *55*(2), 267–306. https://doi.org/10.5305/intelegamate.55.2.0267

Hert, P., & Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, *6*(3), 230–243. https://doi.org/10.1093/idpl/ipw008

Hoofnagle, C. J., van der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: What it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501

International Association of Privacy Professionals. (2019). *IAPP-EY Privacy Governance Report 2019* [Report]. International Association of Privacy Professionals. https://iapp.org/resources/article/iapp-ey-annual-governance-report-2019/

Irion, K. (2020, July 24). Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law [Blog post]. *European Law Blog*. https://europeanlawblog.eu/2020/07/24/schrems-ii-and-surveillance-third-countries-national-security-powers-in-the-purview-of-eu-law/

Kamminga, M. T. (2020). Extraterritoriality. In *Max Planck Encyclopedias of International Law*. Oxford Public International Law. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1040?prd=MPIL

Kant, I. (1796). *Zum ewigen Frieden: Ein philosophischer Entwurf* (Bibliograph. aktualisierte Ausg.). Reclam.

Kantar. (2019). *The General Data Protection Regulation* (Special Eurobarometer, p. 487a) [Report]. European Commission. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/86886

Keller, D. (2018, September 10). Don't Force Google to Export Other Countries' Laws. *The New York Times*. https://www.nytimes.com/2018/09/10/opinion/google-right-forgotten.html

Korff, D. (2021, June 17). Initial comments on the EU Commission's final GDPR adequacy decision on the UK [Blog post]. *Data protection and digital competition*. https://www.ianbrown.tech/2021/06/17/initial-comments-on-the-eu-commissions-final-gdpr-adequacy-decision-on-the-uk/

Kuczerawy, A., & Rauchegger, C. (2020). Injunctions to remove illegal online content under the eCommerce Directive: Glawischnig-Piesczek. *Common Market Law Review*, *57*, 1495–1526.

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). *International Journal of Law and Information Technology*, *18*(3), 227–247. https://doi.org/10.1093/ijlit/eaq004

Kuner, C. (2019). Article 45. Transfers on the basis of an adequacy decision. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp.

771–796). Oxford University Press.

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The Privacy Policy Landscape After the GDPR. *Proceedings on Privacy Enhancing Technologies*, *2020*(1), 47–64. https://doi.org/10.2478/popets-2020-0004

Mantelero, A. (2020). The future of data protection: Gold standard vs. Global standard. *Computer Law & Security Review*, *40*. https://doi.org/10.1016/j.clsr.2020.105500

Mayer-Schönberger, V. (2011). *Delete: The virtue of forgetting in the digital age ; with a new afterword by the author*. Princeton University Press.

Miyashita, H. (2020, July 3). EU-Japan mutual adequacy decision. [Blog post]. *Blogdroiteuropéen*. https://blogdroiteuropeen.com/2020/07/03/eu-japan-mutual-adequacy-decision-by-hiroshi-miyashita/

Padova, Y. (2019). Is the right to be forgotten a universal, regional, or 'glocal' right? *International Data Privacy Law*, *9*(1), 15–29. https://doi.org/10.1093/idpl/ipy025

Petersen, N. (2020). Human Dignity, International Protection. In *Max Planck Encyclopedias of International Law*. Oxford University Press. https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e809?prd=MPIL

Polakiewicz, J. (2021). A Council of Europe perspective on the European Union: Crucial and complex cooperation. *Europe and the World: A Law Review*, *5*(1). https://doi.org/10.14324/111.444.ewlj.2021.30

Powles, J., & Chaparro, E. (2015, February 18). How Google determined our right to be forgotten. *The Guardian*. http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search

Propp, K., & Swire, P. (2020, August 13). After Schrems II: A Proposal to Meet the Individual Redress Challenge [Blog post]. *Lawfare*. https://www.lawfareblog.com/after-schrems-ii-proposal-meet-individual-redress-challenge

RIS - 6Ob195/19y—Entscheidungstext—Justiz (OGH, OLG, LG, BG, OPMS, AUSL), (Oberster Gerichtshof 15 September 2020). https://www.ris.bka.gv.at/Dokument.wxe?Abfrage=Justiz&Gericht=&Rechtssatznummer=&Rechtssatz=&Fundstelle=&AenderungenSeit=Undefined&SucheNachRechtssatz=True&SucheNachText=True&GZ=&VonDatum=&BisDatum=12.11.2020&Norm=&ImRisSeitVonDatum=&ImRisSeitBisDatum=&ImRisSeit=Undefined&ResultPageSize=100&Suchworte=6Ob195%2f19y&Position=1&SkipToDocumentPage=true&ResultFunctionToken=c426c30b-ff1d-49c5-8896-dac2cb78a0c1&Dokumentnummer=JJT_20200915_OGH0002_0060OB00195_19Y0000_000

Rojszczak, M. (2020). Does global scope guarantee effectiveness? Searching for a new legal standard for privacy protection in cyberspace. *Information & Communications Technology Law*, *29*(1), 22–44. https://doi.org/10.1080/13600834.2020.1705033

Rothstein, M. A., & Tovino, S. A. (2019). California Takes the Lead on Data Privacy Law. *The Hastings Center Report*, *49*(5), 4–5. https://doi.org/10.1002/hast.1042

Rustad, M. L., & Koenig, T. H. (2019). Towards a Global Data Privacy Standard. *Florida Law Review*, *71*(2), 365–454.

Ryngaert, C., & Taylor, M. (2020). The GDPR as Global Data Protection Regulation? *American Journal of International Law*, *114*, 5–9. https://doi.org/10.1017/aju.2019.80

Samonte, M. (2020). Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU

Law. *European Papers - A Journal on Law and Integration*, *4*(3), 839–851. https://doi.org/10.15166/2499-8249/332

Sartre, J.-P. (2020). *Being and Nothingness*. Routledge.

Sloot, B. (2014). Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. *International Data Privacy Law*, *4*(4), 307–325. https://doi.org/10.1093/idpl/ipu014

Svantesson, D. J. B. (2019). Article 3. Territorial scope. In C. Kuner, L. A. Bygrave, & C. Docksey (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 74–99). Oxford University Press.

Theil, S. (2017). Is the 'Living Instrument' Approach of the European Court of Human Rights Compatible with the ECHR and International Law? *European Public Law*, *23*(3), 587–614.

Tracol, X. (2020). "Schrems II": The return of the Privacy Shield. *Computer Law & Security Review*, *39*. https://doi.org/10.1016/j.clsr.2020.105484

Tzanou, M. (2020). Schrems I and Schrems II: Assessing the Case for the Extraterritoriality of EU Fundamental Rights. In F. Fabbrini, E. Celeste, & J. Quinn (Eds.), *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Hart Publishing. https://doi.org/10.5040/9781509940691

Ukrow, J. (2018). Data protection without frontiers? On the relationship between EU GDPR and amended CoE Convention 108. *European Data Protection Law*, *2*, 239–247. https://doi.org/10.21552/edpl/2018/2/14

Van Alsenoy, B. (2018). Reconciling the (extra)territorial reach of the GDPR with public international law. In G. Vermeulen & E. Lievens (Eds.), *Data protection and privacy under pressure. Transatlantic tensions, EU surveillance, and big data* (pp. 77–100). Maklu.

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, *7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Worldwide Obligation of Facebook to Cease and Desist from the Publication of Photographs of Dr. Eva Glawischnig-Piesczek in Connection with Defamatory Insults and/or Words of Equivalent Meaning, (Oberster Gerichtshof 15 September 2020). https://www.ogh.gv.at/en/uncategorized/worldwide-obligation-of-facebook-to-cease-and-desist-from-the-publication-of-photographs-of-dr-eva-glawischnig-piesczek-in-connection-with-defamatory-insults-and-or-words-of-equivalent-meaning/

Wybitul, T. (2020, June 24). *Arbeitsgericht Düsseldorf: 5.000 Euro immaterieller Schadensersatz wegen Datenschutzverstößen* [Blog post]. CRonline. Portal zum IT-Recht. https://www.cr-online.de/blog/2020/06/24/arbeitsgericht-duesseldorf-5-000-euro-immaterieller-schadensersatz-wegen-datenschutzverstoessen/

Zwitter, A. (2015). Peace and Peace Orders: Augustinian Foundations in Hobbesian and Kantian Receptions. In H. Gärtner, J. W. Honig, & H. Akbulut (Eds.), *Democracy, Peace, and Security* (pp. 59–80).

Zwitter, A., & Lamont, C. K. (2014). 15—Enforcing Aid in Myanmar: State Responsibility and Humanitarian Aid Provision. In A. Zwitter, C. K. Lamont, H.-J. Heintze, & J. Herman (Eds.), *Humanitarian Action: Global, Regional and Domestic Legal Responses* (pp. 349–374). Cambridge University Press. https://doi.org/10.1017/CBO9781107282100.022

Published by


in cooperation with