CHAPTER 3

Competing Jurisdictions: Data Privacy Across the Borders

Edoardo Celeste and Federico Fabbrini

Abstract Borderless cloud computing technologies are exacerbating tensions between European and other existing regulatory models for data privacy. On the one hand, in the European Union (EU), a series of data localisation initiatives are emerging with the objective of preserving Europe's digital sovereignty, guaranteeing the respect of EU fundamental rights and preventing foreign law enforcement and intelligence agencies from accessing personal data. On the other hand, foreign countries are unilaterally adopting legislation requiring national corporations to disclose data stored in Europe, in this way bypassing jurisdictional boundaries grounded on physical data location. The chapter investigates this twofold dynamic by focusing particularly on the current friction between the EU data protection approach and the data privacy model of the United States (US) in the field of cloud computing.

E. Celeste (✉) • F. Fabbrini
School of Law and Government, Dublin City University, Dublin, Ireland
e-mail: edoardo.celeste@dcu.ie; federico.fabbrini@dcu.ie

T. Lynn et al. (eds.), *Data Privacy and Trust in Cloud Computing*,
Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-030-54660-1_3

Keywords Cloud computing • Data privacy • Data protection • Data localisation • Data residency • Digital sovereignty

3.1 Introduction

Over the past decade, the right to privacy and the protection of personal data have been increasingly recognised as fundamental values at global level (Greenleaf 2019; Bygrave 2014; Solove 2008). Yet, their understanding still varies significantly among jurisdictions. One apparent example is offered by the different approach to data privacy in the European Union (EU) and the United States (US). In Europe, data protection is a constitutionalised fundamental right, and a comprehensive set of legislation has been put in place to make the regulation of personal data processing uniform across member states. Conversely, in the US, data privacy is not explicitly enshrined in the federal constitution, and is regulated only in selected pieces of legislation targeting specific sectors considered worthy of intervention.

Divergence in legal frameworks of data protection is certainly not a novelty of the last decade. However, the recent development of borderless digital technologies, such as cloud computing, amplifies the risk of tensions between different regulatory models. When data are stored in the cloud, it becomes more difficult to identify the applicable law easily. In response to this phenomenon, data localisation initiatives requiring data to be physically stored in servers located within national boundaries have recently emerged as a regulatory trend to avoid conflicts of law, enhance the level of data privacy protection, limit the risk of access from foreign intelligence agencies, and facilitate domestic law enforcement.

This chapter investigates this twofold dynamic by focusing on the current friction between the EU data protection approach and the US data privacy model in the context of cloud computing. The chapter is structured as follows. In Sect. 4.2, we discuss the main areas of divergence between EU and US approach to data privacy. Then, in Sect. 4.3 we explain how these differences create a series of regulatory challenges in the context of cloud computing. Section 4.4 analyses how recent legal and policy developments on both sides of the Atlantic are addressing these issues, with a particular focus on data localisation initiatives and strategies to preserve digital sovereignty. The chapter concludes with the

proposition that data localisation does not represent a panacea for resolving tensions between competing jurisdictions in the field of cloud computing, and that transnational cooperation and effective international agreements are needed now, more than ever.

3.2 Data Privacy Across the Atlantic

In Europe and the US, data privacy law emerged almost simultaneously in the 1970s (Jones 2017). Both legal systems recognise the importance of protecting personal data and the potential risks deriving from a misuse of such data. Yet, on the two sides of the Atlantic, two different regulatory models have emerged in the field of data privacy (Schwartz and Solove 2014; Tourkochoriti 2014).

In Europe, the respect of privacy and the protection of personal data are recognised as fundamental rights. In 1950, as a reaction to intrusive surveillance practices of totalitarian regimes that afflicted Europe in the first half of the twentieth century, the European Convention on Human Rights enshrined the individual right of respect for private and family life, home and correspondence (Article 8). In its case law, the European Court of Human Rights, which is the competent jurisdiction for the interpretation of the Convention, has affirmed that the concept of private life must be construed broadly in order to protect all aspects of human personality, including individual personal data (Council of Europe 2019; Fabbrini 2015). In 2000, the EU Charter of Fundamental Rights explicitly enshrined the right to privacy and data protection in two distinct provisions, Articles 7 and 8, respectively. Although originally lacking binding legal value with the transposition of the Lisbon Treaty in 2009, the Charter was recognised as having a primary legal status in the hierarchy of EU legal sources, at the same level of EU founding treaties (Fabbrini 2015).

The US is often referred to as the cradle of the right to privacy. Back in 1890, Samuel Warren and Louis Brandeis authored a seminal article published on the Harvard Law Review in which they advocated for the recognition of a broad conceptualisation of the right to privacy and the protection of the individual against external intrusions (Warren and Brandeis 1890). However, in contrast to the EU, in the US, at least at federal level, there is no explicit constitutional provision protecting the right to privacy or data protection. Indeed, the US Constitution dates to 1787 and its Bill of Rights was added only three years later, so well before privacy became an issue. The case law of the US Supreme Court

progressively recognised different aspects of privacy, regarded both as a negative right against State intrusion and as a positive right to self-determination in a variety of contexts, including the choice of using contraceptives or terminating pregnancy (Flaherty 1991). Lacking an explicit reference, the US Supreme Court had to find a constitutional support for the right to privacy in the "emanations" and "penumbras" of the Bill of Rights (*Griswold v. Connecticut*, 381 U.S. 484). In particular, they examined the Fourth Amendment, protecting citizens against unreasonable search and seizures (Solove 2001), and the Fourteenth Amendment, subjecting any deprivation of life, liberty and property to due process rules (Cate and Cate 2012).

Besides the different constitutional frameworks, the EU and the US also developed alternative regulatory models in the field of data privacy. Over the past few decades, the EU has introduced a fully comprehensive set of legislation governing the processing of personal data, both in the private and in the public sector (Fabbrini 2015). In 2016, the EU replaced the 1995 Data Protection Directive, which represented the core piece of legislation adopted to harmonise national statutes in the field, with a General Data Protection Regulation (GDPR), whose provisions are directly binding in all member states (Albrecht 2016). Conversely, the US have rejected a similar all-encompassing approach, in favour of exclusively regulating specific sectors which were felt to be more in need of intervention (Schwartz and Solove 2014). Although being a pioneer in the data privacy field, having adopted the Privacy Act 1974, which regulates data processing by federal agencies, the US never introduced a unitary and comprehensive piece of legislation in the field of data privacy, and only few US states have. At the federal level, US data privacy law is a mosaic of normative instruments covering a variety of issues, spanning from children's privacy to the use of data in financial services (Schwartz and Solove 2014).

In Europe, the basic presumption is that processing personal data represents an interference with the right to data privacy that can be tolerated only if it satisfies certain legal conditions. In the US, instead, data processing is considered fully legitimate in so far as it is not prohibited by law, and a strong emphasis is placed on the role of individual consent as a basis to process personal data (Tourkochoriti 2014). European data protection law, in order to reduce the risk of circumvention and ensure an even level of protection across member states, has introduced provisions extending its application to data controllers that are not established in the EU, but

nevertheless process data related to EU residents (Article 3 GDPR; Christopher Kuner 2015; Svantesson 2015; de Hert and Czerniawski 2016). In the US, data privacy statutes do not have a similar extraterritorial effect.

Lastly, in contrast to US legislation, EU data protection law also regulates international data transfers. Article 44 GDPR establishes that personal data can freely circulate among member states, but cannot be transferred to third countries unless they provide an adequate level of protection. Article 48 of the GDPR even explicitly prohibits any data disclosure requested by a foreign authority, unless based on an international treaty. The European Commission can adopt a decision certifying the adequacy of the level of data protection of a third country (Article 45 GDPR). Countries like Israel, Argentina, Uruguay, and recently Japan, have been certified as providing an adequate level of protection (European Commission 2019). Conversely, the Commission has only issued a partial adequacy decision in relation to the United States.

In 2000, the European Commission adopted Decision 2000/520/EC (so called "Safe Harbor") which established the adequacy of US data protection rules: in particular, US corporations that are subject to the supervision of the Federal Trade Commission could self-certify their respect of the Safe Harbor Principles (Greer 2011). However, in the aftermath of the Snowden revelations about the existence of US mass surveillance programmes, this decision was invalidated by the European Court of Justice (ECJ). In the *Schrems* case (C-362/14), decided in 2015, the ECJ held that the Commission, by certifying the adequacy of the Safe Harbor scheme, failed to take into account the power of US law enforcement authorities to access on a generalised basis EU data transferred under the Safe Harbor scheme (Cole and Fabbrini 2016; Padova 2016). According to the ECJ, such a model of bulk surveillance cannot be tolerated as it compromises the essence of the right to privacy protected by the EU Charter of Fundamental Rights (para 94 of the judgment; see Ojanen 2017).

The Safe Harbor scheme was promptly replaced by the so-called "Privacy Shield", which was negotiated between the European Commission and the US authorities in 2016 and entered into force with Decision 2016/1250. The new system is very similar to the Safe Harbor in terms of functioning, but has been accompanied by a series of further guarantees, especially in relation to the individual right of redress (Tracol 2016; cf. Bender 2016). Moreover, after the Snowden revelations, the US started a progressive revision of its law enforcement legislation (Cole and Fabbrini

2016). Nevertheless, recently, a new legal challenge was made against the EU-US Privacy Shield and in July 2020 the ECJ declared also this instrument invalid for breach of EU data privacy law. (Case C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximilian Schrems*). In its ruling, the ECJ emphasized the same problem as in *Schrems I*: the level of protection of EU data in the US is still contested.

The *Schrems I* and *Schrems II* cases both represent examples of circumstances in which the EU and US data protection frameworks enter in conflict. This situation arises when transnational processing of data is involved, and is highly problematic both from a EU and US perspective. On the one hand, EU data protection law imposes limits to the free transfer of personal data to third countries that are not deemed to offer an adequate level of protection of personal data. On the other hand, US authorities are loath of bending their sovereign decisions to EU requests in the field of data privacy as a result of the so-called Brussels effect (Bradford 2012). As the next section will explain, cloud computing, by ordinarily involving transborder data processing, represents a particularly challenging area.

3.3 Regulating Borderless Cloud Computing

Cloud computing denotes "flexible, location-independent access to computing resources that are quickly and seamlessly allocated or released in response to demand" (Hon et al. 2011a, p. 6). This broad definition encompasses three models of cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These models, as is apparent from their denomination, differ on the basis of the service offered, spanning from the mere provision of infrastructure to the supply of software (Hon et al. 2011a). These paradigms, however, are not mutually exclusive. It is conversely possible that a cloud computing service is composed of infrastructure, platform or service layers at the same time (Hon et al. 2011a). Just to mention some familiar examples in the academic context, Dropbox, the Google apps and Microsoft 365 represent commonly used Software as a Service cloud computing services.

A further classification of cloud computing models takes into account their users: one can distinguish between public, private or hybrid cloud computing models (Esayas 2012; see also Varadi et al. 2012). In the first case, cloud computing services are available to the general public, an example being the social network Facebook; in the second case, their use is restricted to a limited number of users, such as in tailored cloud services

for corporations or institutions; lastly, the third case represents an intermediary solution.

Using computing resources which are available in "the cloud" is advantageous for a series of reasons (Hon et al. 2011a; Esayas 2012). First of all, cloud computing can provide services which are tailored to the end user. Secondly, cloud computing can flexibly respond to changes in users' demand. And lastly, but certainly not least, cloud computing is significantly cheaper than developing and maintaining individually owned infrastructure, platforms or software. Those resources are centralised, and thanks to their virtual character, they are shared according to the specific needs of potential users.

From a technical perspective, this is possible thanks to the so-called "sharding" (Hon et al. 2011a). Data are not concentrated in a single virtual cloud, but are fragmented into a series of "shards", replicated, and stored in different locations. This procedure, which is entirely automated, allows the cloud computing service to maximise its performance. On the one hand, smaller pieces of information can be accessed more quickly. On the other hand, their replication enhances the security of the system by reducing the risks of node failures or data loss.

The technical architecture of cloud computing creates a series of challenges from a data protection perspective. First of all, cloud computing providers may be unaware of the fact that they are processing personal data. Hon et al. talk of the "cloud of unknowing" (2011a, p. 1). Secondly, the multi-layered structure of cloud computing services may create issues in relation to the correct identification of the data controller and processor, and the consequent allocation of responsibilities. For example, it has been contended that cloud service providers merely offering infrastructure as a service can even hardly be considered as data processors (Hon et al. 2011b). Thirdly, cloud computing models may involve a continuous transfer of data on a global scale, and therefore potentially interesting a multiplicity of states. The "sharding" procedure, on which cloud computing relies, partitions and transfers data automatically.

The introduction of the GDPR has removed a series of jurisdictional problems existing under the Data Protection Directive. The GDPR is immediately legally binding in all EU member states. As a consequence, at least if the transfer occurs within the EU, the data controller will have one single legislative reference point instead of multiple different domestic pieces of legislation. Moreover, the GDPR has eliminated the reference to the use of equipment situated in an EU member state as a criterion to

define its scope of application. The idea of linking the applicability of EU data protection law to the physical use of an equipment no longer corresponded to the technological reality (Hon et al. 2012; Esayas 2012; Christopher Kuner 2010). The GDPR now regulates data controllers who are not established in the EU, but offer goods or services in the EU or monitor the behaviour of European data subjects (Article 3 GDPR). However, the GDPR has not substantially modified the data transfer regime involving third countries. Therefore, data controllers should still ensure that, when using cloud computing services, European data are not transferred to third countries which do not guarantee an adequate level of protection, or without appropriate safeguards (Hon and Millard 2012).

The existence of these regulatory obstacles to the free flow of personal data from the EU to third countries has led cloud computing providers to offer services storing personal data on servers exclusively located in the EU (Hon and Millard 2012). EU data protection law has been one of the main drivers behind the creation of "regional" clouds besides cross-border ones (Svantesson and Clarke 2010). A tension therefore emerges between, on the one hand, the economic and technological dimensions that push towards the offer of cloud computing services on a global scale in order to maximise efficiency and minimise costs, and, on the other hand, regulatory and policy initiatives that conversely impose boundaries and *de facto* limit the free flow of data for privacy rights reasons. Since the main cloud computing providers are based in the US and, as pointed out above, the EU and US are adopting different approaches in relation to data privacy, this situation raises several challenges. The next section will examine a series of initiatives that are emerging on both sides of the Atlantic to address these problems.

3.4 Data Localisation and Digital Sovereignty

Over the past few years, data localisation—which is the requirement to store data in servers located within a given jurisdiction—has also emerged as a regulatory trend at global level (Mishra 2015; Selby 2017). To mention a successful example, in 2014 Russia introduced a statute requiring citizens' personal data to be stored in the national territory (Hon et al. 2016; Selby 2017). The objectives of these kinds of legislation are disparate. Safeguarding data privacy and ensuring effective law enforcement at domestic level are the two most recurrent explicit justifications of these initiatives (Mishra 2015; Hon et al. 2016). The timing of this

phenomenon, which has thrived after the Snowden revelations about the US mass surveillance programmes, also suggests that data localisation is emerging as a response to the risk of data access from foreign intelligence agencies (Hon et al. 2016).

In Europe too, a series of data localisation initiatives has recently emerged. Since 2011, ideas of a Europe-only cloud, if not even a "virtual Schengen area", have been circulating (Kuner et al. 2015; Hon et al. 2016). In 2013, the German telecommunications operator, Deutsche Telekom announced a plan to create a German "Internetz", by ensuring that traffic data are only routed nationally (Hon et al. 2016). Similarly, after Russia's annexation of Crimea in 2014, Estonia explored the possibility of creating a "data embassy" via a combination of a physical diplomatic seat in a friend country to locate data centres, and a "virtual embassy" in a private cloud to store critical data (Millard 2015).

More recently, the European Commission has launched a European Cloud Initiative in the context of its Digital Single Market Strategy (European Commission 2016). This policy includes the creation of a European Open Science Cloud, which aims to offer European researchers a safe environment to store and share data, and a European Data Infrastructure, which would provide the necessary super-computing solutions. Moreover, in 2019, the German Ministry for Economic Affairs and Energy has officially presented 'Gaia-X', the project for a European federated cloud-based data infrastructure (Federal Ministry for Economic Affairs and Energy (BMWi) 2019).

These initiatives show that the concept of "digital sovereignty" has recently emerged as a common thread in the European debate on data localisation. Originally, proposals such as the virtual Schengen area were politically justified by the need to ensure a sufficient level of security in the digital environment (Hon et al. 2016). The protection of human rights, and in particular the rights to privacy and data protection, has been the second main driver of discussions about data localisation in Europe. In the *Digital Rights Ireland* case, for example, the ECJ invalidated Directive 2006/24/EC, compelling telecommunications operators to retain all users' metadata for a fixed period of time, on the basis, *inter alia*, that it failed to require the storage of personal data in Europe (Digital Rights Ireland 2014, para. 68; Celeste 2019). According to the ECJ, the Data Retention Directive, by allowing telecommunications operators to store retained meta-data outside Europe, undermined the power of member states' national data protection authorities to control data processing, as

expressly prescribed by Article 8(3) of the EU Charter of Fundamental of Rights (Digital Rights Ireland 2014, para. 68; cf. Tele2 Sverige 2016, para. 122).

More recently, in the summer 2019, the data protection authority of the German Land of Hessen temporarily ordered Hessian schools not to use Microsoft Office 365 (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019a; cf. Walden 2011). The decision followed Microsoft's announcement that the company would not ensure data storage on the German cloud only. The supervisory authority found that the risk of allowing US authorities to access European children's data without appropriate guarantees made the use of Microsoft's software unacceptable from a fundamental rights perspective (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019a, para. 2). The Hessian ban, which was originally extended to Google and Apple cloud applications (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019a, para. 5), was subsequently lifted a month later following an intense phase of dialogue with Microsoft. The supervisory authority, however, stated that the investigation would have continued in light of several legal and technical issues still to be solved (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019b).

The first decision of the Hessian data protection authority justified the ban of Microsoft Office 365 to preserve the state's "digital sovereignty" (Der Hessische Beauftragte für Datenschutz und Informationsfreiheit 2019a, para. 2). Digital sovereignty is a concept that permeates the recent debate on data localisation in Europe widely and particularly in Germany. For example, it is the primary goal of the Gaia-X Project launched in 2019 by the German Ministry for Economic Affairs and Energy (Federal Ministry for Economic Affairs and Energy (BMWi) 2019, p. 6). In the Ministry's document, digital sovereignty is defined both as "independence" and as "self-determination" (Federal Ministry for Economic Affairs and Energy (BMWi) 2019, p. 7). Remarkably, this concept is not uniquely linked to the state dimension, encompassing also the power of companies to freely determine the use and structure of their digital systems, data and processes (Federal Ministry for Economic Affairs and Energy (BMWi) 2019, p. 7). In this way, digital sovereignty is presented as a solution to the European dependence from foreign companies and infrastructures, as well as to offer an opportunity to abide by and affirm European values.

Yet, the project of achieving European digital sovereignty is not immune from the typical criticism characterising data localisation legislation

(Mishra 2015). First, implementing a similar policy means increasing costs due to the relocation of data centres and services in Europe, and subverting global economic trends. Moreover, digital sovereignty could not be a panacea vis-à-vis the issue of security. As the Estonian project of creating a virtual data embassy shows, centralising data may enhance the level of vulnerability, while delocalisation, as the sharding procedure in the context of cloud computing services demonstrates, can actually strengthen system resilience. Lastly, initiatives aiming to preserve digital sovereignty are often criticised as ways to conceal a form of protectionism (Mishra 2015; Millard 2015; C. Kuner et al. 2015). Digital sovereignty would not merely lead to a balkanisation of the digital realm for the sake of preserving European fundamental rights, but also to allow European companies to fill the economic gap distancing them from American and Asiatic technology giants.

While Europe is seeking to strengthen its digital sovereignty, however, analogous trends are emerging also elsewhere. In 2018, for example, the US introduced the CLOUD Act, a new legislation enabling US law enforcement authorities to require US corporations to disclose data, independently of their physical location (Abraha 2019). The statute was purposefully adopted as a response to a case in which Microsoft contested a search warrant aiming to gather data stored on its Irish servers (Svantesson and Gerry 2015). Microsoft lamented that, under the Electronic Communications Privacy Act 1986, the US government was not explicitly authorised to serve extraterritorial warrants. The introduction of the CLOUD act in 2018 mooted the dispute against Microsoft, which had meanwhile reached the US Supreme Court (Abraha 2019). The new statute empowers US law enforcement authorities to require data in the 'possession, custody and control' of a US corporation, notwithstanding such information may be physically located outside the US (Abraha 2019).

Data localisation is not just a US and European phenomenon. In 2017, in the context of the increasing trade war with the US, China passed a new National Intelligence Law obliging companies to collaborate with Chinese intelligence agencies (Yang 2019). This legislation produced strong criticism in the US (Lian 2019; The White House 2019; cf. Doffman 2019). Yet it reveals a drift towards growing fragmentation of the digital space to impose national sovereignty, which raises significant challenges for cloud computing.

3.5 Conclusion

Borderless cloud computing technologies are exacerbating existing tensions between EU and US approaches to data privacy. On the one hand, a series of European initiatives are progressively exercising a centripetal force on data held by companies operating in the EU. Their main objective would be to preserve Europe's digital sovereignty by guaranteeing the respect of European fundamental rights and preventing foreign law enforcement and intelligence agencies from accessing personal data of EU citizens and residents. On the other hand, foreign countries are unilaterally adopting legislation requiring national corporations to disclose data stored in Europe, in this way bypassing jurisdictional boundaries grounded in physical data location. Both the US and Chinese recently adopted statutes represent two paradigmatic examples of this trend, and clearly highlight how a conflict between European rules and foreign laws is emerging.

From a European standpoint, it is therefore evident that data localisation alone cannot represent the universal remedy for all the existing risks. In a globalised digital environment, even investigating about a domestic crime may likely entail accessing data held in different jurisdictions. Erecting permanent barriers to the free flow of data could eventually amount to a Sisyphean labour, difficult and ultimately futile. For this reason, enhancing cooperation and establishing more functional agreements with third states, making sure that the protection of digital rights becomes a shared concern transnationally and globally, still seems to be the best choice for the EU.

References

Abraha, H. H. (2019). How Compatible Is the US "CLOUD Act" with Cloud Computing? A Brief Analysis. *International Data Privacy Law, 9*, 207–215. https://doi.org/10.1093/idpl/ipz009.

Albrecht, J. P. (2016). How the GDPR Will Change the World. *European Data Protection Law Review, 2*(3), 287–289.

Bender, D. (2016). Having Mishandled Safe Harbor, Will the CJEU Do Better with Privacy Shield? A US Perspective. *International Data Privacy Law, 6*(2), 117–138. https://doi.org/10.1093/idpl/ipw005.

Bradford, A. (2012). The Brussels Effect. *Northwestern University Law Review, 107*(1), 1–67.

Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford: Oxford University Press.

Cate, F. H., & Cate, B. E. (2012). The Supreme Court and Information Privacy. *International Data Privacy Law, 2*(4), 255–267. https://doi.org/10.1093/idpl/ips024.

Celeste, E. (2019). The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios. *European Constitutional Law Review, 15*(1), 134–157. https://doi.org/10.1017/S1574019619000038.

Cole, D., & Fabbrini, F. (2016). Bridging the Transatlantic Divide? The United States, the European Union, and the Protection of Privacy across Borders. *International Journal of Constitutional Law, 14*(1), 220–237. https://doi.org/10.1093/icon/mow012.

Council of Europe. (2019). Guide on Article 8 of the European Convention on Human Rights. Retrieved from https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf

de 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.

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2019a, July 9). Stellungnahme des Hessischen Beauftragten für Datenschutz und Informationsfreiheit zum Einsatz von Microsoft Office 365 in hessischen Schulen. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. Retrieved from https://datenschutz.hessen.de/service

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. (2019b, August 2). Zweite Stellungnahme zum Einsatz von Microsoft Office 365 in hessischen Schulen. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit. Retrieved from https://datenschutz.hessen.de/pressemitteilungen/zweite-stellungnahme-zum-einsatz-von-microsoft-office-365-hessischen-schulen

Digital Rights Ireland. (2014). ECLI:EU:C:2014:238. ECJ.

Doffman, Z. (2019). Trump's Huawei Ban Rejected by New Ruling in Germany. *Forbes*, 15 October. Retrieved from https://www.forbes.com/sites/zakdoffman/2019/10/15/trumps-huawei-ban-rejected-by-surprise-new-report/.

Esayas, S. Y. (2012). A Walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of "Processing" and "Transferring" Personal Data. *Computer Law & Security Review, 28*(6), 662–678. https://doi.org/10.1016/j.clsr.2012.09.007.

European Commission. (2016). *European Cloud Initiative—Building a Competitive Data and Knowledge Economy in Europe*. COM(2016) 178 Final. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016DC0178&from=EN

European Commission. (2019). Adequacy Decisions. Text. European Commission—European Commission. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Fabbrini, F. (2015). The EU Charter of Fundamental Rights and the Rights to Data Privacy: The EU Court of Justice as a Human Rights Court. In S. de Vries, U. Bernitz, & S. Weatherill (Eds.), *The EU Charter of Fundamental Rights as a Binding Instrument* (pp. 261–286). Hart.

Federal Ministry for Economic Affairs and Energy (BMWi). (2019). Project GAIA-X—A Federated Data Infrastructure as the Cradle of a Vibrant European Ecosystem. Retrieved from https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/project-gaia-x.pdf?__blob=publicationFile&v=4

Flaherty, D. H. (1991). On the Utility of Constitutional Rights to Privacy and Data Protection. *Case Western Reserve Law Review, 41*, 831–855.

Greenleaf, G. (2019). *Global Data Privacy Laws 2019: 132 National Laws & Many Bills*. SSRN Scholarly Paper ID 3381593. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=3381593

Greer, D. (2011). Safe Harbor—A Framework That Works. *International Data Privacy Law, 1*(3), 143–148. https://doi.org/10.1093/idpl/ipr010.

Hon, W. K., Millard, C., Singh, J., Walden, I., & Crowcroft, J. (2016). Policy, Legal and Regulatory Implications of a Europe-Only Cloud. *International Journal of Law and Information Technology, 24*(3), 251–278. https://doi.org/10.1093/ijlit/eaw006.

Hon, W. K., Hörnle, J., & Millard, C. (2012). *Data Protection Jurisdiction and Cloud Computing—When Are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing, Part 3*. SSRN Scholarly Paper ID 1924240. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=1924240

Hon, W. K., & Millard, C. (2012). *Data Export in Cloud Computing—How Can Personal Data Be Transferred Outside the Eea? The Cloud of Unknowing, Part 4*. SSRN Scholarly Paper ID 2034286. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=2034286

Hon, W. K., Millard, C., & Walden, I. (2011a). *The Problem of "Personal Data" in Cloud Computing—What Information Is Regulated? The Cloud of Unknowing, Part 1*. SSRN Scholarly Paper ID 1783577. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=1783577

Hon, W. K., Millard, C., & Walden, I. (2011b). *Who Is Responsible for "Personal Data" in Cloud Computing? The Cloud of Unknowing, Part 2*. SSRN Scholarly Paper ID 1794130. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=1794130.

Jones, M. L. (2017). The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood. *Social Studies of Science, 47*(2), 216–239. https://doi.org/10.1177/0306312717699716.

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J. B., & Lynskey, O. (2015). Internet Balkanization Gathers Pace: Is Privacy the Real Driver? *International Data Privacy Law, 5*(1), 1–2. https://doi.org/10.1093/idpl/ipu032.

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 1). *International Journal of Law and Information Technology, 18*(2), 176–193. https://doi.org/10.1093/ijlit/eaq002.

Kuner, C. (2015). Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law. *International Data Privacy Law, 5*(4), 235–245. https://doi.org/10.1093/idpl/ipv019.

Lian, Y.-Z.. (2019). Opinion | Where Spying Is the Law. *The New York Times*, 13 March, sec. Opinion. Retrieved from https://www.nytimes.com/2019/03/13/opinion/china-canada-huawei-spying-espionage-5g.html

Millard, C. (2015). *Forced Localization of Cloud Services: Is Privacy the Real Driver?* SSRN Scholarly Paper ID 2605926. Social Science Research Network, Rochester, NY.

Mishra, N. (2015). *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?* SSRN Scholarly Paper ID 2848022. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=2848022

Ojanen, T. (2017). Rights-Based Review of Electronic Surveillance after Digital Rights Ireland and Schrems in the European Union. In D. Cole, F. Fabbrini, & S. Schulhofer (Eds.), *Surveillance, Privacy and Transatlantic Relations* (pp. 13–29). Hart.

Padova, Y. (2016). The Safe Harbour Is Invalid: What Tools Remain for Data Transfers and What Comes Next? *International Data Privacy Law, 6*(2), 139–161. https://doi.org/10.1093/idpl/ipw009.

Schwartz, P. M., & Solove, D. J. (2014). Reconciling Personal Information in the United States and European Union. *California Law Review, 102*, 877–916. https://doi.org/10.2139/ssrn.2271442.

Selby, J. (2017). Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both? *International Journal of Law and Information Technology, 25*(3), 213–232. https://doi.org/10.1093/ijlit/eax010.

Solove, D. J. (2001). Digital Dossiers and the Dissipation of Fourth Amendment Privacy. *Southern California Law Review, 75*(5), 1083–1168.

Solove, D. J. (2008). *Understanding Privacy*. Cambridge, MA: Harvard University Press.

Svantesson, D., & Clarke, R. (2010). Privacy and Consumer Risks in Cloud Computing. *Computer Law & Security Review, 26*(4), 391–397. https://doi.org/10.1016/j.clsr.2010.05.005.

Svantesson, D., & Gerry, F. (2015). Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond. *Computer Law & Security Review, 31*(4), 478–489. https://doi.org/10.1016/j.clsr.2015.05.007.

Svantesson, D. J. B. (2015). Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation. *International Data Privacy Law, 5*(4), 226–234. http://dx.doi.org.ucd.idm.oclc.org/10.1093/idpl/ipv024.

Tele2 Sverige. (2016). ECLI:EU:C:2016:970. ECJ.
The White House. (2019). Executive Order on Securing the Information and Communications Technology and Services Supply Chain. The White House, 15 May. Retrieved from https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/
Tourkochoriti, I. (2014). The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-E.U. in Data Privacy Protection. *University of Arkansas at Little Rock Law Review, 36*, 161–176.
Tracol, X. (2016). EU–U.S. Privacy Shield: The Saga Continues. *Computer Law & Security Review, 32*(5), 775–777. https://doi.org/10.1016/j.clsr.2016.07.013.
Varadi, S., Kertesz, A., & Parkin, M. (2012). The Necessity of Legally Compliant Data Management in European Cloud Architectures. *Computer Law & Security Review, 28*(5), 577–586. https://doi.org/10.1016/j.clsr.2012.05.006.
Walden, I. (2011). *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*. SSRN Scholarly Paper ID 1781067. Social Science Research Network, Rochester, NY. Retrieved from https://papers.ssrn.com/abstract=1781067
Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review, 4*(5), 193–220. https://doi.org/10.2307/1321160.
Yang, Y. (2019). Is Huawei Compelled by Chinese Law to Help with Espionage? *Financial Times*, 5 March. Retrieved from https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0