J U R I D I C U M

Legal access to data

The Cloud Act in relation to the GDPR

Maja Tägt

VT 2021

RV600G, Rättsvetenskaplig kandidatkurs med examensarbete, 30 högskolepoäng, delkurs 3
Tillämpade studier, 15 högskolepoäng
Examinator: Joakim Nergelius, Jesper Ekroth, Rigmor Argren
Handledare: Petra Hietanen-Kunwald
Antal ord i brödtext: 14036

Summary

This paper examines whether the compatibility of an order, issued under the US Cloud Act to obtain information stored within the Union, is permissible under Article 49 of the EU GDPR. It finds that the Commission and the European Data Protection Board (EDPB) reaches the same conclusions regarding warrants to obtain information issued under the Cloud Act, but in different ways. It concludes that such orders may be compatible with the EU GDPR provided that certain criterions are satisfied.

Keywords: GDPR, Cloud Act, datatransfer

Table of Contents

Abbreviations

Cloud Act	Clarifying Overseas Use of Data Act
EU	European Union
ECPA	Electronic Communications Privacy Act
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
FTC	Federal Trade Commission
GDPR	General Data Protection Regulation
MLAT	Mutual Legal Assistance Treaty
NIST	National Institute of Standards and Technology
US	United States of America
WP29	Working Party Article 29

1. Introduction

1.1 Background

A combination of high-capacity networks, low-cost computers, and storage devices together with autonomic utility computing have led to a rise in demand in the usage of cloud computing. The file hosting service Dropbox reported 15 million paid users in 2020.[1] The benefit of cost-effective data storage alternatives for both the service provider and the individual, is that the individual does not need specialised hardware knowledge, whilst the provider can utilise economies of scale and run the system from one central site. Legal questions emanate however as companies may be governed by one state law, have subsidiaries in another state whilst servers are spread across multiple states with potential users in a different state altogether. The traditional location– the jurisdictional approach – has proven slow and difficult to manage, because by the time law enforcement has obtained relevant judicial documents the data has either been moved or deleted.

Privacy and data protection issues have emerged, catalysed by revelations of Edward Snowden in 2013, when he released documents proving US law enforcement conducted massurvelliance on a global scale, and fuelled further by the Cambridge Analytica scandal, where manipulation of personal data affected elections, shaking democracy to its core. It prompted European legislators to tighten laws on dataprotection to ensure data within the Union is safe from manipulation and surveillance programmes, which resulted in a stricter GDPR than initially proposed.[2] It is considered to be the most progressive take on dataprotection on a global scale, and few legal orders can match it. In the aftermath of these scandals, individuals demand their data to be protected from unauthorised parties', at the same time law enforcement requires access to stored data on the cloud for criminal investigations to avoid impunity and fears the internet might go dark because it cannot access evidence stored in the cloud, whilst tech companies have interest in not losing revenue. But what does it mean for law enforcement access to evidence?

In the aftermath of the scandals, individuals demand their data to be protected from unauthorised parties', at the same time law enforcement requires access to stored data on the cloud for criminal investigations to avoid impunity and fears of the internet might go dark, whilst tech companies have interest in not losing revenue.

The United States approach manifests through the Clarifying Lawful Overseas use of Data (the Cloud Act)[3] and which enables US law enforcement to access stored data outside the US, whilst the European Union recognises the high level of dataprotection through the General Data Protection Regulation (GDPR).[4]

[1] Dropbox, 'Fourth Quarter and Fiscal results 2020' <https://investors.dropbox.com/news-releases/news-release-details/dropbox-announces-fourth-quarter-and-fiscal-2020-results> accessed 20 May 2021.
[2] Augustín Rossi, 'How the Snowden Revelations Saved the EU General Data Protection Regulation' (2018) The international spectator Vol. 53 No.4 104-6.
[3] the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943)
[4] European Commission Regulation on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ 2 L 119/01

1.2 Purpose and research questions

The United States of America (US) enacted the Cloud Act to enable law enforcement to access data stored overseas. It sparked controversy and privacy activists argue it infringes on state sovereignty and the right to privacy. This thesis' purpose is to analyse whether the act of US law enforcement to obtain information stored in the Union is in accordance with Article 48 or 49 of the GDPR. To fulfil this purpose the thesis will have one main research question, with two sub–question which are as follows:

1. Can a request for obtaining information under the US Cloud Act compatible with the requirements set out in Article 48 European GDPR?
   1.1 If Article 48 cannot be applied, is there any applicable derogations under Article 49 GDPR?
   1.2 How can the tests applied under the Act be ensured under Article 47 of the Charter?

1.3 Methodology and materials

In order to achieve the purpose of the thesis, the legal dogmatic method will be used. By applying this method, relevant sources of law are identified. The purpose of this method is to systematise norms, laws, rules, and legal norms that is applicable to an area of law.[5] The aim is to identify any discrepancies in the law and establish relationships between the relevant material[6] to determine *de lege lata*. The material must be weighed against each other, taking into account the hierarchy and authority of the material, whilst understanding its context and interpretation.[7] The thesis takes primarily a European, and a *de lege lata* perspective and does not claim to resolve or suggest changes to current law which is why the classic legal dogmatic method proves useful.

For the purpose of this thesis, the main source of law will be EU legislation, The Clarifying Lawful Overseas Use of Data (the Cloud Act)[8] and, the General Data Protection Regulation (GDPR).[9] Both primary and secondary union law will be examined. Primary Union law consists of the founding treaties, consolidated in the Lisbon Treaty[10] with protocols and amendments. Data protection and the right to privacy are rights enshrined in EU since the Lisbon treaty[11] entered into force 2009, making the Charter of the Fundamental Rights (the Charter)[12], and the Convention of Human Rights (ECHR)[13] part of EU law. It means that the GDPR must be read in light of the

[5] Jan M. Smits, 'What is Legal Doctrine? On the aims and methods of legal-dogmatic research' (2015) 2015/06 Maastricht European Private Law Institute 5.
[6] Ibid.
[7] Ian Dobison, Francis Johns, 'Qualitative Legal Research' *in* Mike McConville, Wing Hong Chui (eds.) *Research Methods for Law* (Edinburgh University Press 2007).
[8] the Clarifying Lawful Overseas Use of Data Act or CLOUD Act (H.R. 4943)
[9] European Commission Regulation on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (2016) OJ 2 L 119/01
[10] Consolidated Version of the Treaty on European Union [2008] OJC115/13.
[11] Consolidated Version of the Treaty on European Union [2008] OJ C115/13.
[12] Charter of fundamental rights of the European Union [2012] OJ C326/391.
[13] European Council, The Convention on the Protection of Human Rights and Fundamental Freedoms [1950] OJ C103/27.

Charter, as the right to dataprotection and the right to privacy are recognised fundamental rights recognised in the Union.

Law produced through institutions exercising the powers conferred to them make up secondary union law. It consists of Directives, Regulations and Decisions[14] which will be examined. Additionally, soft law sources will be used to provide context and understanding to the Cloud Act and the GDPR. Doctrine from the technology sector have been used to define the technological elements of the thesis.

1.4 Delimitations

The nature of legal tech is constantly developing, as demanded by technological advancements. Naturally, there are many initiatives from the legislator that has been excluded in the work of this thesis as they are yet to be implemented. Negotiations are ongoing between the US and the EU to conclude an agreement under the Cloud Act, which has been left out of the thesis completely as currently, any conclusions drawn from published material is to be incorrect as the material is probably likely to change before its final publication. A conclusion on available material would be inaccurate and irrelevant by the time the agreement is implemented.

A proposed ePrivacy Directive published by the Commission aims to update existing privacy laws within the Union, but as it is still in its proposed state, any analysis of it would have a *de lege feranda* approach and would not provide a correct conclusion, why the decision to exclude it was taken.

The Convention on Cybercrime is not scrutinised in detail, despite its objective to combat cybercrime. It would entail a wider perspective than the European perspective of this thesis. It must be mentioned however that the Budapest Convention is mentioned in relation to the Cloud Act, and in Chapter 7 because the Act mirrors some language to the convention, and the US Congress used the Convention as one of the criteria's that is set out to determine if a government is qualified under the Cloud Act.

1.5 Definitions

Definitions presented in this section are meant to provide context and aid the reader understand key terminology. The definitions provided are limited to what is relevant for the present thesis, but other definitions may exist.

Datacontroller is a natural private entity, public authority, agency, or other body which determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Dataprocessor is a natural or private entity, public authority, agency, or other body which processes personal data on behalf of a controller.

[14] Klaus–Dieter Borchardt, *'The ABC of EU Law'* (2017) Publication's office of the European Union 91.

Processing entails means any act which is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

An exporter is an actor that exports data over the Union border for the purpose of processing, whilst an importer of data is a natural or legal person that imports data from across the Union border for the purpose of processing it.

1.6 Disposition

The thesis starts by defining the Cloud according to accredited industry standard to introduce an uninitiated reader what the Cloud is. The following chapter titled *Dataprotection* presents the reader with arguments why dataprotection matters, consequences for unprotected data to subsequently present the dataprotection standards encompassed under Union law, namely the GDPR. Instead of sections 3.3 throughout 3.6 being located under Chapter 4 titled GDPR, it aims to alleviate the readers understanding of the Cloud Act. Chapter 4 complements Section 3 what is found under Chapter 3, and the Chapter 6 discusses how the Cloud Act and the GDPR may work together. Conclusion of the thesis is found under Chapter 7.
cannot

2. Cloud services

2.1 Introduction

In order to understand what 'the Cloud' entails, a descriptive chapter is presented of how the cloud may be used according to National Institute of Standards and Technology (NIST).[15] In order to understand the Cloud a basic level of understanding of the Cloud is necessary. Lastly, its characteristics and its service models will be presented.

2.2 Definition of the cloud according to NIST

NIST defines cloud services as:

> *"*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. *"*[16]

NIST have identified five essential necessary characteristics. Firstly, the cloud service must provide *on demand self-service*. The user can unilaterally provision computing capabilities, such as server time and network storage as needed, automatically without requiring interaction with the service provider.[17] Secondly, broad network access is required. The service is accessible over the network (internet) and can be accessed through standard mechanisms such as mobile phones, computers, or tablets.[18] The third requirement demands *recourse pooling*, where the user has no detailed knowledge or control over the location of the provided recourses.[19] The consumer should not have to negotiate deals with each service provider, and thus do not need to know the infrastructure of the service. The fourth criteria, *rapid elasticity*, entails that the user can use less or more of the service and the service should appear to have a sense of unlimited capabilities to the user.[20] The service should appear infinite to the user. The fifth, and last characteristics relates to *measured service.* Resource usage by the user can be monitored, controlled, and reported by the provider providing transparency for both the user and the provider.[21] It can be determined either through a pay–per–per usage or charge–per–use basis.

2.2.1 Service models according to NIST

The NIST definition identifies three types of cloud service models. Focus for the present paper is the Software as a Service (SaaS) model, which according to NIST is an application that is available to a user accessible via various client devices, either a web browser, or a program interface.[22]

---

[15] Peter Mell, Timothy Grance, 'The NIST definition of Cloud Computing: Recommendations of the National of Standards and Technology' (2011) NIST Special Publication 800-145 2.
<https://csrc.nist.gov/publications/detail/sp/800-145/final> accessed 31 March 2021.
[16] Ibid 2.
[17] Ibid.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.

The two other models are platform as a service (PaaS) which enables the user to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, or services.[23] The user does not have control over the essential infrastructure but may have control over the deployed applications and possibly limited control over settings for the application hosting environment.[24]
Infrastructure as a Service (IaaS) is the capability provided to the consumer to vest over processing, storage, networks, and other fundamental computing recourses. The user does not control the underlying essential infrastructure, such as the hardware. The user may however control the operating system, storage, deployed applications have possibly limited control of select network components.[25]

2.3 The GDPR Article 49 and its relation to the Cloud

The GDPR codifies the right to protection of data and privacy recognised under EU law by providing procedural steps and a framework for entities processing personal data. It must be lawful under Article 6 GDPR, and it applies to any data that is processed within the Union, and the processing EU persons personal data. The GDPR is relevant for potential transfers to the US via the Cloud under the Cloud Act as the GDPR applies to 'processing' which occurs whenever data is stored, transferred, systemised, organised.

In the absence of other transfer tools Article 48 regulate situations where transfers may occur. If Article 48 does not apply, possible derogations under Article 49 may be triggered, if the data transfer is in line with general principles enumerated in Article 49(2) GDPR.

[23] Ibid 3.
[24] Ibid.
[25] Ibid.

3. Dataprotection

3.1 Introduction

Following section introduces the reader to the data collection that occurs and exemplifies why data protection is important by showing what conclusions can be drawn from a person's messages and gives examples on how it can be misused. On the other hand, it exemplifies why data must flow for criminal investigations to obtain evidence stored on the cloud.

3.2 Importance of dataprotection

The right to privacy is not a 'new' right. It has just evolved and adapted over time, namely the age of digitalisation. Samuel D Warren and Louis Brandeis wrote in the Harvard Review about 'the right to be left alone' as a response to the times' invasion of privacy; the unauthorised circulation of private portraits and the interference by the newspapers, to name a few, called for development of the right of the person.[26] The right of the person to determine to what extent their thoughts, sentiments and emotions are communicated to others is a right secured to each person, and each person has the authority to fix the limits of publicity of personal sentiments, thoughts and emotions. No other has the right to publish or make public the private domain without his or her consent.[27] Although written about two centuries ago, the remarks made then are applicable in the era of digitalisation as the same questions are being asked and similar issues are present. As most fundamental rights, it stems from a natural law standpoint and the justifications are generally moral, but also considered part of a healthy, functioning democracy.[28]

The increasing role of digitalisation and technology in human life and information collected is however unprecedented. The rapid growth of collecting and storing data is a result of automated data generators and collected by machines or sensors which can collect detailed data by the minute.[29] It is commonly referred to as 'Big Data' because of the sheer volume collected. Digital information poses new challenges in particular regard to privacy as information is transferred across borders with "ease, speed, and unpredictability", and there is a "psychical disconnect between the data and the user".[30]

A woman using the dating app 'Tinder' requested information that was kept about her to be released to her. She received 800 pages of interaction, detailed messages she sent and received with geographical location and timestamps, photos, times of login and persons she had connected with.[31] Once data is sorted and put in context to the user it becomes *useful* information.[32] The timestamps, messages or connections about persons using the app is not useful unless it is connected to a person. For example, from the woman's data, her sexual preference could be determined based on the persons she connected with (sex, origin, skin colour, age etc), her

[26] Samuel D. Warren, Louis D. Brandeis, 'The Right to Privacy' (1890) Harvard Law Review Vol. 4 No. 5 195
[27] Ibid 199.
[28] Paul M. Schwartz, 'Privacy and Democracy in Cyberspace' (2000) 52 Vand. L. Rev. 1609.
[29] Jonas Flodén, *Essentials of Information Systems* (Studentlitteratur 2018) 85.
[30] Jennifer Daskal, 'The Un-Territoriality of Data' (2015) The Yale Law Journal 125:326.
[31] Judith Duportail, 'I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets' (26 September 2017) <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold> accessed 10 May 2021.
[32] Jonas Flodén, *'Essentials of Information Systems'* (Studentlitteratur 2018) 10-11.

personal interests and opinions could be determined based on messages sent and interactions she's had, and her geographical movements could be tracked based on the geographical tags of where she psychically logged in and where she used the app.
The Tinder example is only one example of how data is collected and stored on individuals using software. It is useful for companies providing services to collect and analyse the data of its users for business purposes, amongst things to develop their product– but one must ask, how much do companies know about their users, and how are they are using the information?

Facebook for example, has become one of the world's largest media corporation without producing any content themselves.[33] Free to use for persons, the company sells ads based on personal information of its users to advertisers on the premise the information is anonymised to the advertisers.[34] To exemplify how it might work, a hypothetical advertiser may pay Facebook to advertise their product only to females between the ages between 18-35, in a specific geographical area that have specific interest. Facebook then displays the advertisements to those specified by the vendor. It is called 'targeted ads', it can be positive for companies to increase revenue but for individuals it might feel intrusive.

The company Cambridge Analytica gathered information through Facebook on about 87 million users – without user authorisation – in order to target them for political campaigns using a highly sophisticated machine.[35] Cambridge Analytica referred to it as an 'extra-secret sauce' of how to successfully win political campaigns.[36] In short, ads generated by psychographically tailored predictions would send microreinforcing messages to 'targets' i.e. groups of persons, to reinforce their world beliefs in order to influence them to vote, or supress the vote for competitions. The codename 'Project Alamo' was coined when Cambridge Analytica was hired for the election campaign of President Trump.[37] A whistle-blower came forward about the illicit and misuse of personal data and it was a global scandal. The tools had been used in all areas of the world to influence elections.[38] The misuse of data is said to be a serious threat to democracy.[39] Trained impersonal system monitors have the ability to shape human actions and can, with small tweaks, potentially influence the outcome of political elections, without the user realising it.

In 2013, Edward Snowden, a former employee of NSA, leaked documents about National Security Agency (NSA) surveillance and revealed the secret cooperation of many US based

[33] Sam Levin, 'Is Facebook a publisher? In public it says no, but in court it says yes' (3 July 2018) <https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit> accessed 10 May 2021.
[34] Facebook terms of use accessed 16 April 2021.
[35] Jim Isaak, Mina J. Hanna, 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection' (2018) IEEE Computer Society 57.
[36] Alex Hern, 'Cambridge Analytica: how did it turn clicks into votes' (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 10 May 2021.
[37] Rikard. Lindholm, 'Project Alamo's Data-driven Ads on Facebook won Trump the Election' (Semantiko 19 February 2017) <https://semantiko.com/project-alamo-trump-facebook-ads> accessed 16 April 2021.
[38] All places where SCL claim success. Devjyot Ghoshal, 'Mapped: The breathtaking global reach of Cambridge Analytica's parent company' (28 March 2018) <https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/> accessed 10 May 2021.
[39] Jamie Bartlett, '*The People Vs Tech: How the Internet is killing democracy (and how to save it)*' (Edbury digital 2018).

companies with the authorities' clandestine activities. It prompted many to turn away from US based services, resulting in companies with American connection losing up to an estimated $180 billion USD.[40] Consequently, in an effort to not lose revenue, particularly US based companies market and implement models of their product to assure those concerned with authority surveillance that is does not occur.[41]
Why data protection matters are hence multifold; it is a selling point for companies to concerned consumers, it prevents information being misused or manipulated by illicit actors, it empowers individuals to know how their information is used, and it protects individuals' right to be free from unauthorised interference in their correspondence, but for many it is a moral standpoint.

3.3 Why data needs to flow

Challenges inherent in cybercrime evolve quickly as technology creates those challenges. European Union Agency for Cybersecurity (ENISA) identified 15 top threats 2019-2020. Malware[42], web-based attacks[43], and (spear) phishing[44] is at the top. Identity theft[45], information leakage[46] and ransomware[47] are assessed as increasing threats. ENISA noted the impact the pandemic continues to have on technology; it forced large scale adoption of technology to master various critical aspects of the pandemic, ranging from coordination of health, to remote learning for schools to the international response to the pandemic.[48] With most persons either working or studying from home, usage of the Cloud has increased.

Crimes that require a physical element have moved online entirely or are partly facilitated online communications. For example, terrorism, human– and drug trafficking have a technological element to them.[49] Children are particularly vulnerable on the Internet. Through harassment, systematic abuse and verbal, psychological and psychical violence children can be manipulated for various ill-intended reasons, which often result in long lasting damage to their health and

[40] Clint Boulton, 'NSA's Prism Could Cost IT Service Market $180 Billion' Wall Street Journal (16 August 2013) <https://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion/> accessed 10 May 2021.
[41] Paul M Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Columbia Law Review 1681.
[42] Malicious software. Aims to disrupt service, obtain information, conduct identity theft or espionage. ENISA, 'From January 2019 to April 2020 Malware' ENISA Threat Landscape.
[43] Increasing complexity of web applications creates challenge to protect them against outside or inner threats. Example: SQL Injection (SQLi).
[44] Phishing is fraudulent attempt to steal user data, ex login details, credit card information using social engineering techniques. Spear phishing relies upfront on research of the victim making it one of the most successful types of attacks. See further ENISA, 'January 2019 to April 2020 Phishing' ENISA threat Landscape 2.
[45] Illicit use of victim's personal identifiable information by impostor to impersonate the victim to gain financial benefit. ENISA, 'From January 2019 to April 2020 Identity theft' ENISA Threat Landscape 2.
[46] Data for which an organization is responsible for is subjected to security breach resulting in breach of confidentiality, availability, or integrity. Frequently causes information leakage which is one of the biggest cyber threats. See further ENISA, 'Information leakage from January 2019 to April 2020' ENISA Threat Landscape 2.
[47] Where ill-intended actors attempt to harm governments, businesses, and persons daily. Usually by blocking usage of a computer or software until ransom has been paid. See further ENISA, 'Ransomware from January 2019 to April 2020' ENISA Threat Landscape 2.
[48] ENISA, 'The year in review from January 2019 to April 2020' ENISA Threat Landscape 8.
[49] Europol, 'A corrupting influence: The infiltration and undermining of Europe's economy and society by organized crime' EU Socta 2021 – Serious and Organized Crime Threat Assessment 41.

development, which can lead to self-harm or suicide.[50] Europol recently raised concerns over a rise in live long distance child abuse cases because of lockdowns means.[51]

Cybercrime has limited risk of detection and prosecution due to the inherent difficult nature to investigate, but even if the illicit actor was successfully prosecuted the sentences are generally low.[52] Which leads to criminals acting with impunity, victims may not get justice and illegal actions to soar which means that the internet may continue to be a lawless arena where crimes soar and goes unpunished.

3.4 Dataprotection and privacy as part of EU law

Relevant for present thesis is Article 7 and 8 of the Charter. Article 7 of the Charter protects the individual's right to: i) the private life, autonomy of individuals ii) the right to family life iii) home and iv) correspondence.[53]

Article 8 of the Charter reads: "everyone has the right to the protection of personal data concerning him or her".[54] Whilst the Charter explicitly protects the right to privacy and dataprotection, Article 8 ECHR does not explicitly mention it, its scope have been expanded by the European Court of Human Rights (ECtHR).[55] The right to privacy is protected as a general principle of EU law[56] This means that the principles underpinning the right to privacy and dataprotection must be taken into account when applying or creating EU law as it enjoys higher privileges and authority then other EU law.

Article 47 of the Charter entails that everyone whose rights and freedoms guaranteed by the law of the Union has the right to an effective remedy before an independent and impartial tribunal.[57] Legislation that does not ensure individuals with the right to an effective remedy concerning his or her data does not protect the essence of the fundamental right in Article 47.[58]
Although the two rights are connected and might overlap, they are not the same. The right to privacy concerns what and how entities that collects data can use it, whilst dataprotection ensures there are safeguards to restrict access from unauthorised parties to the data.

3.5 Conceptualising data protection under Union law

Dataprotection is the control and safeguards implemented to keep data safe from unauthorised or illicit use and are codified in the GDPR (hereafter the Regulation).
There are six main principles underpinning the GDPR and they are codified in Article 5. This section will state them and briefly explain what they entail and why they matter for the protection of data.
The principles are: 1. Lawfulness, fairness, and transparency. 2. Purpose limitation 3. Data minimisation. 4. Accuracy. 5. Storage limitation. 6. Integrity and confidentiality.

---

[50] Ibid.
[51] Although data is fragmented.
[52] (n 49).
[53] (n 12) Article 7.
[54] Ibid Article 8.
[55] *Rotaru v Romania* App no 28341/95 (ECtHR, 4th May 2000) para 43.
[56] 136/79 *National Panasonic v Commission* [1980] ECR 2033 para 17.
[57] Case C-279/09 *DEB Deutsche Energihandels- und Beratungsgesellschaft mbH* [2010] I-13849.
[58] (n 12) Article 47.

Principle one has three components to it, as the concepts are clearly linked. In order for the processing to be transparent, the concerned person must be informed about what processing will be conducted. The factual processing must correspond to the description provided to the datasubjects, i.e., it must be fair, and the processing cannot violate the law. Recital 60 expands on this notion stating that the person should be "informed of the existence of the processing operation".[59]

Paragraph two specifies that data within the scope of Article 8 must be processed fairly for specified purposes and on the basis of the consent of the individual.[60] If these conditions are met, there is no interference with the right to dataprotection.[61] Article 13(1)(d) of the DPD can be ground for such justification, as it allows for data processing in criminal investigations.

3.6 Justified interferences of dataprotection and the right to privacy

As the right to data protection is a fundamental right it encompasses high level of protection. Limitations to the right may only occur if it is provided for by law, respects the essence of the right, is proportionate, necessary, and genuinely meet the objectives of general interest recognised by the Union or the need to protect rights and freedoms of others under Article 52 of the Charter.[62] It is however not an absolute right and must be considered in relation to its function in society, be balanced against other fundamental rights and must be proportionate.[63]

The principle of accountability entails that controllers and processors must actively ensure compliance with the Regulation by implementing legal, technical and organised measures and be transparent with these efforts with datasubjects, the general public and dataprotection supervisory authorities.[64] The accountability principle applies likewise to transfers that occurs to third countries[65] since they are considered data processors.[66] The ECJ established in the Schrems II[67] case that the level of protection afforded to datasubjects within the Union must be read in light of the Charter and must be guaranteed irrespective of the legal basis for the transfer to a third country.[68] If a processor or controller does not comply with, or can no longer ensure the level of protection encompassed in Union law the contract between them must be terminated.[69] There must be a collaboration between the exporter and importer of data in its performance of responsibilities by information for example of any development affecting the level of protection of the personal data received in the importers country.[70]

In relation to law enforcement access to severe interference with the right, the Court have

[59] (n 4) Recital 60.
[60] (n 9) Article 8(2).
[61] Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063 para 49.
[62] (n 50) Article 52(1).
[63] Case C-507/17 *Google LLC, successor in law toInc v Commission nationale de l'informatique et des libertés* [2016] OJ C 347 para 60.
[64] (n 7) Article 5(2) and Article 28(3)(h).
[65] Ibid Article 44, Article 47(2)(d) and Recital 101.
[66] (n 36) para 45.
[67] (n 36).
[68] (n 36) paras 92–3.
[69] Ibid paras 134–142.
[70] Ibid para 134.

established that the only interference to the right of privacy and data protection must be targeted, proportional to the offence and the crime investigated must be of serious nature.[71] Additionally, the interference must be objectively pursued via legislation and a serious interference may be justified in areas of prevention, investigation, detection and prosecution of criminal offence that constitutes 'serious'. Less severe interferences however might be justified in the same areas by the objective to prevent, investigate, detect, and prosecute 'criminal offences generally'.[72]

The ECJ ruled in an opinion, where the Union entered into agreement with Canada with the aim to collect and retain data of travellers from the EU to fight terrorism.[73] The agreement permitted Canadian border force to be sent personal information about travellers coming into Canada, such as name, passport number, travel time and dates were sent from the private flight company ahead of flights. It obliged Canada to retain data for five years, the immediate masking of sensitive data, laid out requirements of rights and access to and correction and erasure of data, and for the possibility of administrative and judicial redress for Union citizens.[74]

The court noted that taken as a whole, the travel data may reveal complete travel plans, information can be sourced about the passengers, existing relationships between individuals, information on the financial situation of its passengers and their dietary habits, or state of health. It may even provide other sensitive information about air present passengers. The fact that the data generally was analyzed systematically via automated means before the passengers arrived in Canada, may additional information on the private life of the passengers. The fact that the data may be retained for up to five years makes it possible that sensitive information on the private life of passengers is stored and available for a time longer than is necessary.[75] The Court thus found an interference with the rights found in Article 7 and 8 of the Charter.

In its assessment whether the interference could be justified, the Court noted that parts of the agreement could not be limited to what was strictly necessary to combat terrorism. The rules were not clear nor precise, and it found that the retaining of data after the data passenger had left Canada lacked legal basis and was not limited to what was strictly necessary as regards to passengers that were identified of not posing a terrorist threat.[76] After such passengers left Canada, there was not a sufficient link between the travelers and the threat of terrorism that would justify holding their data for longer than necessary. Most importantly, the Court ruled that the rules on sharing data with non–EU countries were not sufficiently clear and requested that data may only be shared when there is an agreement in place or a decision of the Commission permitting such transfers. The Court thus concluded that the transfer of personal data to a third country constitute processing, which is subject to Union law.

In relation to this thesis, it can be understood that a transfer to a third state where an interference cannot be justified violates Union protection principles. Both in the Schrems II case and in the Canadian case, the safeguards put in place of the data's destination was not found to be sufficient.

[71] Joint cases C-203/15 and C-698/15 *Tele2 Sverige and Watson and Others* [2016] ECLI:EU:C:2017:222 para 99.
[72] Case C–207/16 *Ministerio Fiscal* [2018] EU:C: 2018:788, para 54.
[73] Opinion by the Court 1/15 [2017] ECLI:EU:C:2017:592
[74] Ibid.
[75] Ibid.
[76] Ibid.

4. GDPR

4.1 Introduction

The GDPR covers all of EU residents and organisations within the Union, but also any organisation that are trading with the EU or target EU residents. Under the Regulation, the European Data Protection Board (EDPB) was created and given greater legal authority than its predecessor Working Party 29 (WP29). The guidelines issued by WP29 complement the EDPB. Six fundamental principles underline the Regulation which are: fairness, lawfulness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.[77] It aims to empower the user by increasing transparency for individuals to why their data is stored and how it used, whilst holding processors and controllers accountable. Organisations that fail to comply with the provisions set out the Regulation may face fines up to either €20,000,000 or 4% of the global annual turnover. Whichever is appliable depends on which is greater for the private entity at hand. This chapter lays out the procedural requirements under the Regulation and why it is relevant for the thesis. Notably, it applies to a US based company that offers services in the Union.

4.2 Material scope

The GDPR applies to any processing that occurs of personal data either entirely or partly by automated means.[78] Although the definition is not codified, the caselaw by the ECJ and the ECHR provide what constitutes as processing. Relevant for this paper is the Canada and the Schrems II[79] case. Processing for the purpose of Union law include transfer to a third country. Special category of special data under the Regulation is any data that may identify ethnical origin, political or religious beliefs, data concerning health or sexual orientation.[80] It is in line with the case law originating from the ECJ and the ECtHR but expands on the rights of the datasubjects. Amongst tings, under the Regulation, datasubjects have the right to be forgotten which entails the datasubjects right to ask a service provider to delete all information that it stored about him or her.[81] Individuals also have the right to object to the processing of data concerning him or her if it can be found it is not necessary.[82]

4.2.1 Lawful processing

To the question whether the processing is lawful or not, one or more of the criteria set out in Article 6 must be fulfilled. The lawfulness does "…not per se require a legislative act adopted by parliament, but the legal basis or legislative measure should be clear and precise and its application should be foreseeable to persons subject to it".[83] Article 6(1)(a) explicitly presents that a person must have consented to the processing of his or her personal data, or a civil law contract could be entered into between the data subject and the data controller.[84]

[77] (n 4) Chapter 5.
[78] Ibid Article 3.
[79] Case C-311/18 Schrems v Data Protection Commissioner [2020] ECLI:EU:C:2020:559
[80] (n 4) Article 9.
[81] Ibid Article 17.
[82] Ibid Article 21.
[83] Ibid Recital 41.
[84] Ibid Article 6(1)(b).

Principle two, that of purpose limitation entails that data can only be collected for specified, explicit and legitimate purposes.[85] The person who's data is collected should be informed of how the data will be used and the processing should be limited to only include what is necessary to meet the purpose set out by the organisation.[86]

4.3 Territorial scope

Through Article 3(1) is the territorial scope established. It specifies that the Regulation is applicable to "the processing of data in the context … of an establishment of a controller or processor in the Union, regardless of where the processing takes place". The wording says it does not matter where the processing takes place, but if the organisation is established within the Union, it is under obligation to adhere to the Regulation. It also applies to organisations not established within the Union, but where a MS law applies by virtue of public international law.[87] One of two criterions must be fulfilled in order for the Regulation to apply: either through the 'establishment' criterion[88] or through the 'targeting' criterion.[89] For the purpose of the Regulation, an establishment implies "the effective and real exercise of activity through stable agreements".[90] Article 3 does not however provide a definition of 'establishment'. The concept of establishment is interpreted broadly; the legal form of for example a branch or subsidiary is not the determining factor of what constitutes an establishment. The court have established a three-legged test: i) is there excursive of real and effective activity – even a minimal one? ii) is the activity through stable arrangements? and iii) is personal data processed in the context of this activity?[91] The test was established in the *Weltimo*[92] case and is still applied to determine what constitute for the purpose of the Regulation.[93] A private entity that provide cloud services to European persons would fall within in the material and territorial scope of the GDPR, therefore the GDPR is applicable to an order issued under the Cloud Act even if an order regards only the stored data on a server within the Union.

4.4 Personal data in relation to the dataprotection

Personal data for the purpose of the GDPR is data which relates to an unidentified or identified person. Any data. It can be cookies[94] from a website to metadata[95] but it can also include situations where data have been anonymised, but the identity of the person can be deduced from the circumstances.[96] to The ECtHR have the most extensive case law regarding dataprotection and the right to privacy, and the ECJ stared to establish caselaw in 2009 on the matter when the Charter became part of EU law. It is therefore relevant for the Regulation, as it provides scope and

[85] Ibid Article 5(1)(b).
[86] IT Governance privacy team, *EU General Data Protection Regulation: An Implementation and compliance guide* (4th edn, IT Governance Publishing 2020).
[87] (n 4) Article 3(3).
[88] Ibid Article 3(1).
[89] Ibid Article 3(2)
[90] Ibid Recital 22.
[91] Case C-230/14 *Weltimo S.R.O. v Nemezeti A Datvelmi Es Informacioszabadsagh Atosag* (Hungarian DPA) [2015] EU:C:2015:639 paras 29-31.
[92] Ibid.
[93] EDPB, 'Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), (12 November 2019) 6.
[94] A cookie tracks the movement of a user on a website.
[95] The data about data, which is timestamps of the data, geographical location, size etc.
[96] Case T-259/03 *Nikolau v. Commission* [2007] OJ C-264

definitions. The caselaw from the ECtHR are more substantive compared to the ECJ because the right to privacy have been recognised under the ECHR for a longer period.

Had the GDPR been enforce at the time of the Cambridge Analytica scandal, the company would have faced a greater fine under it. Facebook would have been fined for not keeping the data safe enough, and Cambridge Analytica would have been fined for unlawful processing of personal data. The definition of personal data under GDPR corresponds to the definitions established by the ECJ, and it could be said that the GDPR essentially codifies what has been found by the ECJ. Any order under the Cloud Act will generally constitute as personal data for the purpose of the GDPR because the definition of personal under the Regulation is wider than what the Act provides.

5. The Cloud Act

5.1 Introduction

The Clarifying Lawful Overseas Use of Data Act (hereinafter the Act) targets serious crimes, including terrorism, sexual violence and crimes against children and was enacted by US Congress 2018. By many it is seen as a paradigm shift in the approach of jurisdiction. Traditionally, jurisdiction has belonged to where the data was psychically stored on the server, but this is approach has proven difficult for several reasons. Data is not a psychical object one can touch, and it can be stored simultaneously on different servers, and by the time a court order or warrant have been issued for a specific location, the data might have been transferred elsewhere or removed. Purpose of the Act is to amend the outdated Stored Communications Act (SCA) and the main rationale is to combat serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime.[97]

The Act consists of two parts. Part I provide for how and when law enforcement can obtain information from service providers. Part II enables the US Attorney General to conclude bilateral agreements with foreign states who meet the criteria set out in the Act to streamline data and circumvent the cumbersome Mutual Legal Assistance Treaty (MLA) process. Traditionally when law enforcement requires stored information in another country, an MLAT process provide a framework for cooperation in cross border criminal investigations where law enforcement send requests to the receiving state asking for cooperation in investigations, whilst ensuring procedural guarantees and safeguards via treaties. It respects state sovereignty by permitting the receiving state to refuse cooperation and is grounded on diplomatic relations, but it is a slow and cumbersome process that is not fit for the digital age.[98] On both sides of the Atlantic statistics shows it takes on average up to ten months to process one request.[99]

The amount of evidence accumulating on the internet, and the number of requests that occur combined with the slow process have raised the demand for a faster, less cumbersome process. The American response is part II of the Cloud Act. It creates a framework for cross border transfers, where domestic law applies firstly and is supplemented by international agreements and principles.[100] A warrant to obtain information is hence based on American domestic law.
The purpose of the act is multifold; to end impunity for serious crimes committed online, simplify the process for foreign authorities to obtain stored data in another country criminal investigations, in some situations circumvent the MLAT process and provide a procedural step to resolve situations where service providers face conflicting legal obligations.
For the purpose of this thesis, only part I of the Cloud Act will be analysed. Part II will briefly be mentioned, particularly the possibility to enter into agreements with foreign governments as it is

[97] US Department of Justice, 'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (White Paper, April 2019) 2.
[98] Els De Busser, 'The Digital Unfitness of Mutual Legal Assistance' (2017) Security and Human Rights 28 161
[99] Letter from Assistant Attorney Gen. Peter Kadzik to Vice-President Joseph R. Biden, President, United States Senate (July 15, 2016) <https://www.aclu.org/sites/default/files/field_document/doj_legislative_proposal.pdf> accessed 15 April 2021.
[100] Marcin Rojszzack, 'CLOUD act agreements from a EU perspective' (2020) Computer law & Security Review 105442.

relevant for the discussion of protection of data. It allows private entities to share data they have previously under US law been prohibited to provide to foreign governments.

5.2 Prior to the Act

There was an ongoing case in the United States of America Supreme Court (US Supreme Court) between Microsoft and the US government on whether Microsoft had a legal obligation under SCA to disclose a customer's email correspondence who was believed to be engaged in illegal drug trafficking.[101] Microsoft provided law enforcement with the timestamps of the email but not the content of the emails, as the content was stored on servers in Ireland and Microsoft argued SCA warrants did not have extraterritorial reach. Before the case was ruled on in the highest court, the US Congress enacted the Cloud Act amendment that codified the extraterritorial reach of SCA warrants. The Microsoft Ireland case was mooted, and it handed over the contents of the correspondence to law enforcement.

The Act amends the Stored Communications Act (SCA) which is part of the umbrella law Electronic Communications Act (ECPA).[102] The SCA regulate conditions in which private entities may disclose information to other entities or to law enforcement, and how data is stored.

5.3 Material scope of the Cloud Act

In a response to law enforcements fears that the internet might "go dark", the purpose of the Act is to lower the threshold and enable a faster process by law enforcement to access information.[103] It aims to respond to the revolution of technical advancement by authoring law enforcement to seek information directly from the service provider, but it must go through a court process to minimise intrusive measures. Depending on what data is sought different criteria apply. For example, accessing data stored for less than 180 days, a warrant issued from a judge is required[104] and the authority seeking it must be able to prove 'fair probability' that evidence of the crime exists.[105] Communications stored for longer than 180 days and are non–content information[106] require a court order which were lower standard of 'probable cause' is demonstrated.[107]

5.4 Territorial scope of the Cloud Act

The act stipulates that:

> "…electronic communication services (ECS) and remote computing services (RCS) providers must comply with the obligations of the SCA to preserve, backup, or disclose the contents of a wire or electronic communication … within such providers possession, custody or control, *regardless of whether such communication is located within or outside the United States*".[108]

The extraterritorial jurisdiction principle was however already applied under the SCA, with the traditional test of "control, not location".[109] Entities must however be under 'personal jurisdiction' of the US, which is the question whether a non–US person or company have

[101] United States v. Microsoft Corp., 584 U.S. (2018).
[102] ECPA, 18 U.S.C. § 2702.
[103] Section 102 (2) CLOUD Act.
[104] 18 U.S.C. § 2703(a).
[105] United States v. Perkins, 850 F. 3d 1109, 1119 (9th Cir. 2017).
[106] Non–content data such as IP-adresses, and email correspondence, See Electronic Communications Privacy Act
[107] 18 U.S.C. § 2703(b).
[108] 18 U.S.C. § 2713 § 103(a) (2018).
[109] Matter of Marc Rich & Co., A.G. v. United States, 707 F.2d 663 (2d Cir. 1983).

sufficient contacts with a 'forum' i.e., the US, to be subject to its jurisdiction. It must be determined on the particular facts of each case.[110] Consequently, the service provider may not necessarily be established in the US, but it might still be, depending on the factual case, subject to US jurisdiction by simply offering services to the US market.[111] In order for a warrant to be issued under the Cloud Act, both personal jurisdictions must be applicable, and the "possession, custody or control" test must be fulfilled.

5.5 Possession, custody, or control test

The Cloud Act renders location of data immaterial and instead makes the test of "possession, custody, or control"[112] the *locus* of accessing data.[113] Any provider subject to US personal jurisdiction must comply. What the test entails however is not provided for in the Cloud Act, but the legal text mirrors the language of the Convention on Cybercrime[114] (hereinafter the Budapest Convention).[115] The Budapest Convention is the first Convention to address cybercrime, adopted by the Council of Europe to fight cybercrime on a global scale, which main objective is "to pursue a common criminal policy aimed at the protection of society against cybercrime, by adopting appropriate legislation and foster international co-operation".[116] The Convention is used as a tool under the Cloud Act to streamline data as the Convention. The DOJ argues that parties to the Budapest Convention are, and have been, required to enact domestic laws under Article 18(1) of the Budapest Convention to facilitate cross border cooperation and justifies Section 103 of the Cloud Act by referring to the Budapest Convention.[117] Multiple amicus briefs in the Microsoft case contested this interpretation, and it has been criticised. But since the case was not decided on its merits, the interpretation have not been clarified. This thesis will not go further in it analyse of this controversy but will borrow guidelines from the Budapest Convention regarding the possession, custody or control test as the same language is used under the Cloud Act.[118]

In order to be granted a warrant, US courts apply the 'control test' one in either two ways; a) the 'legal rights' test or b) the 'practical ability' test.[119] For the 'legal rights' test to be applicable, the entity must have the legal rights to obtain documents on demand,[120] Regardless of the *practical* ability to access it.[121] It might however not be so straightforward.

Ordering an entity to procure documents it does not have the legal right to will be futile, preciously because the party does not have a legal way to procure the information.[122] The

---

[110] Winston Maxwell, Mark W Brennan and Arpan A Sura, 'Demystifying the US CLOUD Act: Assessing the Law's Compatibility with International Norms and the GDPR' (Hogan Lovells White Paper, January 2019) 12.
[111] (n 97) 8.
[112] See quote in section 3.1
[113] Chapter 121 of title 18, United States Code § 2713.
[114] Council of Europe, the Convention on Cybercrime (2000) ETS No. 185.
[115] Ibid Article. 18.
[116] Explanatory Report to the Convention on Cybercrime ETS No. 185 para 175.
[117] (n 97) 7.
[118] (n 116) 175.
[119] Johnathan D Jordan, 'Out of "Control" Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent?' (2016) 68 Baylor Law Review.
[120] US v. Int'l Union of Petro. Indus. Wkrs 870 F.2d 1450 (9th Cir. 1989).
[121] In Re Citric Acid Litigation 191 F.3d 1090, 1106 (9th Cir. 1999).
[122] Ibid.

practical ability test have been identified as "the legal right, authority, or *practical ability* to obtain the materials sought upon demand" regardless of the company legal rights to do so.[123] Which means that if the entity have the ability to enter a server in its system, it has do to so regardless of its other contractual obligations.

Courts apply a multifactorial analysis which is takes the facts of each case into account.[124] What the "control" encompasses for the purpose of the Cloud Act remains to be known. Possession and custody amount to psychical possession of the material and is mirrored in the Budapest Convention, but what constitutes as 'control' has no uniform standard.[125] 'Possession or control' for the purpose of the Budapest Convention compelles states to enact legislative acts that would enable respective law enforcement to "order a person in their territory to submit specified computer data in that person's *possession or control*".[126] In the explanatory report to the Budapest Convention 'possession or control' refers to the psychical data concerned in the ordering Party's territory. For example, if a person is issued with a production order for stored information, he or she must procure such information.[127] Merely a technical ability to procure stored information however not within the persons legitimate control does not per se constitute 'control'.[128] Under the Budapest Convention, to apply the practical ability test without regard to the *legal rights* to access the data is not a correct interpretation. Relying on the explanatory report, both the 'practical' and 'legal' test must be fulfilled under the Convention, but under US law one of the two tests is likely to be applied.

Despite the aim to make it easier to access information, the 'possession, custody, or control' test might not entail a straightforward application as it may not take the company structure into account. For example, customers in Germany demand control over their data, and the main selling point to users is the location.[129] Microsoft Germany have a "Data Trust Model". The structure of a data trust model is that servers of that cloud is located in one territory. The servers of Microsoft Germanys are solely located in Frankfurt and Magdeburg and a Data Trustee is contracted to manage and access the data. The Data Manager – Microsoft – solely provide network and hardware whilst the Data Trustee – T-Systems – has the exclusive ability to access and control data. The data is encrypted, only T-Systems has the keys and Microsoft can only access the servers in limited instances, for example to conduct maintenance of the servers under strict supervision of T-Systems.[130] T-system is also point of contact for data requests under foreign law, as the trust agreement is a contract between the companies under German law which generally restricts the access of Microsoft.[131] As a result, Microsoft have neither practical access

[123] Dietrich v. Bauer 198 F.R.D. 397 (S.D.N.Y. 2001).
[124] (n 110) 13.
[125] Haleform H. Abraha, 'Regulating law enforcement access to electronic evidence across borders: the United States approach' (2020) Information & Communications Technology Law, 29/3 333.
[126] (n115) Article 18.
[127] (n 116) para 173.
[128] Ibid.
[129] Peter Sayer, 'For Germany's Cloud Providers, It's Location, Location, Location' (2016) Network World http://www.networkworld.com/article/3043951/for-germanys-cloud-providers-its-location-location-location.html <accessed 12 May 2021>.
[130] (n 41).
[131] Frank Simorjay, Microsoft, Microsoft Cloud Germany: Compliance in the Cloud for Organizations in EU/EFTA. (2016) <https://gallery.technet.microsoft.com/Cloud- Germany-Compliance-4161 d8df/file/159647/4/Microsoft%2OTrustee%20Compliance% 20model.pdf> accessed 20 May 2021.

to the data nor the legal right to access it. This is a disadvantage of the Cloud Act as the possibility to reach data stored in such a cloud would be extremely limited, or not possible at all. On the other hand, it is a way for consumers not wanting law enforcement to access their data to sort of protect it. The Cloud Act would not be effective the on such cloud infrastructure as it does not target or understand Cloud structures. The Act might however be effective against other infrastructures.

Google uses the Data Shard Cloud, the type of cloud that breaks data into components, or shards, that is stored both internationally and domestically.[132] The shards are via automated systems sent around the globe and different shards stored at different servers in different jurisdictions.[133] For example, one shard may be stored one day in a datacentre in Finland, automatically moved the next day to Singapore or Chile and the day after that to Belgium. Without all the shards collected and put together at once to form the actual document, the information is an incohesive code of nonsense. Shards are useless on their own. Google can therefore not determine the location of data at a given time.[134] In the Google Pennsylvania case the judge had to instead consider where the access point to the information was located.[135] As he observed: "No one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location have been identified".[136] For Magistrate Judge Reuter it boiled down to (1) where Googles the access point to the data was physically located and (2) where the data would be given to US law enforcement.[137] If the US would be the answer to both points, Google had to surrender.
Considering the overall purpose for the Act to simplify the process for law enforcement to obtain data, the 'control' test ultimately boils down to the cloud infrastructure and contractual obligations of the provider and is not always straightforward.

5.5.1 Nationality and residence test

The 'nationality and residence' requirement is corresponding to the Acts overall purpose to shift jurisdictional *locus*, whilst at the same time ensuring state sovereignty compliance towards other states. The requirement to challenge an order only if the person is not a US-person does however imply that the nationality or location of the person is known to the service provider.
Service providers does not necessarily verify or collect information of its user's nationality. Microsoft explained in the *Microsoft* case that some providers, amongst them Microsoft, determine the location of its users in the registration process, where the user is asked its geographical location from a dropdown menu. The location provided by the user is then assigned a code where it is scanned in Microsoft backend automatic software to determine which data centre is the closest to the user.[138] Microsoft, as noted by the Second circuit, does not verify user identification or location but simply takes the information provided by the user at 'face value'.[139] Without the verification of nationality, or residency, legal questions emerge. Can a service provider that does not verify or certainly know the nationality or residency of a person challenge a request on the premise it knows its nationality or residency? What happens if a service provider

[132] 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).
[133] See 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).
[134] 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017).
[135] 232 F. Supp. 3d at 725.
[136] 232 F. Supp. 3d at 725.
[137] See 232 F. Supp. 3d 708, 723 (E.D. Pa. 2017) 721-2
[138] Petition for Writ of Certiorari at 14–18, United States v. Microsoft, No. 17-2-01 (US 23 June 2017).
[139] Per Curiam No. 17–2 United States, V. Microsoft Corp. (584 U. S., 17 April 2018).

does disclose the communications of a non–US person to American law enforcement? Paul Schwartz demonstrates how the importance of nationality and residence creates incentives for service providers to accurately collect and store this information to avoid legal reprisals.[140]
It prompts the question, as has been suggested by Paul Schwartz, that service provider may adopt a "know-your-customer" approach, similar to the obligations imposed on bank institutions to collect and process data and report any suspicious behaviour to the authorities. It would ultimately be at the expense of data privacy.

5.5.2 Material risk of violating a qualifying governments law

The second requirement enables service providers to challenge a request within fourteen days if it has 'reasonable belief' to run a 'material risk' to violate a qualifying government law.[141] This raises the question of the actual possibility of challenging a request. It's a burdensome task for service providers to a) find out the nationality of the targeted person and b) cumbersome to determine if the warrant may violate the laws of the foreign country. The fourteen-day time limit imposed on providers poses practical challenges; is that enough time for a service provider that generally does not hold records of its user's nationality, to find that out? The threat of sanctions may incentivise the service provider to simply comply with the order without performing any checks on the information it realises.
The imposed time limit can be extended with the consent of the government or authorised by a court.

5.6 Possibility to quash warrant

For a challenge to quash an issued warrant, two sets of conditions must be met. Only a service provider in receipt of the warrant have access to potentially quash it, on the premise that a bilateral agreement under the Act exists. Two criteria's must be satisfied: "1) the required disclose would cause the provider to violate the laws of a *qualifying* government 2) based on the totality of circumstances, the interests of justice dictate that the legal process should be modified or quashed; and 3) the customer or subscriber is not a US person and does not reside in the US."[142] It does not require an analyse of the targets best interest.
A qualifying government is for the purpose of the Act is a government that have entered into an agreement under the Act with the US. Service providers possibility to challenge an order is therefore extremely limited. Individuals cannot under the Act challenge a request at all.

5.7 Dataprotection in the US under the Cloud Act

The Cloud Act (hereinafter the Act) does not permit individuals to challenge an order for their data. The only possibility to challenge a court order for data is provided to the service providers if they have reason to believe that the data sought after does not relate to a US person. However, only on the premise that a bilateral agreement is in place between the US and the government of the person. Hence, the possibility to challenge a court order to obtain information is extremely limited for both the service provider and the individual. The Act explicitly states that law enforcement must only intentionally target the information of US persons, but it does not provide clarification if EU persons are collateral damage.

---

[140] (n 40).
[141] 18 USC. s 2703 Section 103(b).
[142] 18 U.S.C. § 2703(h) 2018 Appropriations Act, at div. 5, § 103(b).

The judicial recourse for EU persons is possible under Stored Communications Act (SCA), on which the Cloud Act is based upon. It applies to persons which are "any employee, or agent of the United States or any state … and any individual, partnership, association, joint stock company, trust, or corporation".[143] It prohibits unlawful access to stored communications by prohibiting and penalizing whoever who intentionally accesses information without authorisation, or with intent exceeds approved authorisation.[144] Under the SCA, the EU person can start civil processing's in case of unlawful access to their data.[145] But a prerequisite to such possibility is that the person knows about the unlawful collection of data in the first place. It imposes a burdensome task on the individual as it is not certain he or she will which is a substantive obstacle as the Act does not impose an obligation on service providers to do so. There are substantial obstacles for the EU person seeking redress, how does he or she know which state, or court have jurisdiction over the matter?

In 2016, relating to the Schrems II[146] case, it was found that the data of EU persons were likely to be subject to US law enforcement surveillance programmes without providing redress for the individual pursuant to Article 47 of the Charter.[147] The Attorney General is granted the possibility to surveillance and intercept information about persons that are not US citizens under the PRISM surveillance programme, which may also subject the data to Federal Bureau of Investigation (FBI) and the Central Intelligence Agency (CIA).[148] Under the UPSTREAM programme, NSA have the authority to copy and filter data directly from the hardware providing it, i.e., network cables, switches and routers regarding non-US nationals. It has access to metadata and content of the communications concerned.[149] By accessing the underwater cables in the Atlantic, NSA can access data, collect it, and retain it before it reaches American jurisdiction and be subject to any statute.[150] It found the redress available to EU citizens as inadequate, as EU citizens are not covered by the Constitutional 4th Amendment protection, which prohibits "unreasonable searches and seizures" by the US Government.[151] Substantial obstacles exists for EU persons seeking redress. *Locus standi* is considered 'excessively difficult to satisfy and the Court finds that the activities carried out by NSA – by copying datatransfers before it reaches US jurisdiction – are not subject to judicial oversight, is not regulated by statute and are not justified.[152].

The rights guaranteed under Article 7 and 8 of the Charter are however not absolute rights and interferences may be justified. The Court applies a three-pronged test codified in Article 52(1) of the Charter to determine whether there has been an interference. 1) is the interference prescribed by law, or in accordance with the law and does it protect the essence of the right? 2) does it pursue a legitimate aim recognised by the Union? and, 3) is it necessary and proportional i.e., is it the least intrusive measure available in a democratic society to achieve objects or to protect the

[143] 18 U SC §2510.
[144] 18 USC §2701 (a).
[145] ECPA, 18 U.S.C. § 2702
[146] (n 79).
[147] Ibid para 56.
[148] Ibid para 60-1.
[149] Ibid para 62.
[150] Ibid para 63.
[151] United States v. Verdugo-Urquidez, 494 U.S. 1092 (1990).
[152] (n 79) para 65

freedoms of others?[153] In the Schrems II case, the Court found that the surveillance was not prescribed by any statute, did not protect the essence of privacy as it was untargeted, general surveillance of persons and the programme does essentially not contain limitations.[154] It also found a lack of judicial redress for EU persons essentially similar to EU law guaranteed by Article 47 was insufficient.[155]

[153] *Liberty and others v. the United Kingdom* App No. 58243/00, (ECtHR, 1 July 2008) para 58.
[154] (n 79).
[155] C-311/18 (Schrems II), para 169-197

6. Transfers under the GDPR

6.1 Datatransfers to the US based on Article 48 GDPR

In this section, the compatibility between the Cloud Act and the GDPR will be analysed. Any transfer to a third country must comply with the principles set out in Chapter V and have a legal basis under Article 6 the Regulation.[156] The provisions aim to ensure protection afforded to residents is not undermined, and conditions require specific safeguards to be implemented and on the premise that datasubjects rights and effective legal remedies are available.[157] One of the risks with transnational data transfers from one jurisdiction to another is that the protections afforded under EU law is undermined.[158] Article 48 stipulates that transfers to a third country is not authorised by Union law unless it is based on an international agreement, such as an MLAT. It states:

> Any judgment of a court or tribunal … of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable … if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State".[159]

An order issued under American law, such as the Cloud Act, does therefore not have any legal bearing or authority within the Union under Article 48 as it is based on US domestic law and not based on an agreement. The Commission and the EDPB both argued for this in the Microsoft case, both stating that the preferred way of transfer is through an MLAT as such process ensures dataprotection and legal standards are upheld.[160] The EDPB also clarified that private entities faced with an issued warrant under US law should refer US law enforcement to the appropriate MLAT and notify the EDPB of such situation.[161]

6.2 Applicable derogations under Article 49

Article 49 however may provide derogations where a transfer might be permissible in such instances. Its title is "derogations for specific situations" and relevant in the situation of transfers to America is subparagraph (1)(d) of Article 49 that permit transfers if the transfer is found necessary for 'public interest'.[162] It states:

> "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third

[156] EDPS-EDPB Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU–US Agreement on cross-border access to electronic evidence < https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en> accessed 23 May 2021.
[157] (n 4) Article 44
[158] Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (OUP, Oxford 2013) 103.
[159] (n 4) Article 48.
[160] Ibid Article 49(2).
[161] (n 157) 7.
[162] (n 4) Article 49(d).

country or an international organisation shall take place only on one of the following conditions: … the transfer is necessary for important reasons of public interest".[163]

It must be a public interest recognised by Union or MS law[164] and not an interest decided by an American court. The title suggests the provisions may only be used in specific, limited situations. Article 49(2) confirms this as a transfer cannot be systematic, concern specific data of limited datasubjects and cannot require "blanket" transfers of data. A question regarding transfers under the Cloud Act will depend on how repetitive they are in nature. Although Cloud Act requires procedural requirements to be overview by an American Court, the provision Article 49(2) does not permit the transfer to become the rule. It was confirmed by the Commission in the Microsoft case. The question left unanswered because there is limited to no data available on the frequency and volume of requests issued directly to service providers.

In the *Microsoft Ireland* case, the Commission contributed with Amicus curiae brief where it clarified those crimes recognised under Article 83 Treaty of Functioning of the European Union (TFEU) falls within the scope of public interest for the purpose of Article 49(1)(d) GDPR.[165] Amongst identified interests, 'serious crimes' would qualify under 'public interest'. Whether it is the role of a foreign court to assess whether the situation at hand would constitute as a serious crime, the Commission does not clarify on this statement. It does seem like a positive interpretation and transfers may in limited instances be permissible. The Commission thus opens the door to transfers of information based on domestic law in relation to serious crimes that have a cross-border element to them.[166] The Commission emphasise however that any derogation cannot be carried out in a systematic manner, so the derogation becomes norm.[167]

The EDPB on the other hand states that it not sufficient for a third country to issue an order based on domestic law which serves a public interest that "in an abstract sense, also exists in Union or MS law".[168] If a third country require a transfer for investigation purposes to combat any serious crime enumerated in Article 83 TFEU, the existence of a separate legal instrument recognising such crime does not automatically trigger Article 49(1)(d) GDPR applicability.
How one might understand the EDPB in this unclear clarification, the factual transfer must serve the best interest of either the Union or a MS, *as well* as serving the interest of the third country. It further goes on to state that the existence of an international agreement which recognise a particular objective may be an indicator when assessing the existence of a recognised public interest pursuant to Article 49(1)(d), on the premise that the Union or a MS is party to the agreement.[169] This argument seems to loop back to Article 48, that a transfer is not permissible

[163] Ibid.
[164] EDPS-EDPB Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU–US Agreement on cross-border access to electronic evidence < https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en> accessed 23 May 2021.
[165] Brief of the European Commission in United States of America v. Microsoft Corporation, Supreme Court of the United States, no. 17-2, 15-16
[166] Brief of the European Commission in United States of America v. Microsoft Corporation, Supreme Court of the United States, no. 17-2, p. 15-6.
[167] Case C-119/12 *Probst v. mr.nexnet GmbH* [2012]ECLI:EU:C:2012:748 para. 23.
[168] EDPB, 'Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/673' (2018) 10.
[169] Ibid.

unless it is based on an international agreement. A service provider needs to also to consider the strict necessity of the transfer.

A service provider faced with a warrant issued under domestic US law might find itself in a burdensome situation as it must balance three interests, assuming there is an agreement between the requesting country and the other. On the one hand it might sell its products or service to customers on the premise it will not disclose information to law enforcement, or legally prevented from accessing the cloud. At the same time, if they are to challenge an order it has fourteen days to retrieve data might be time-consuming depending on the cloud used, whilst figuring out the nationality and residency of said user and at the same time determining if the transfer is in the best interest of the Union or MS. On the one hand, the provider is American jurisdiction and under legal obligation to procure the evidence that is required and might face reprisals under US law if it does not comply, which is a real probability depending on the cloud structure. On the other hand, it must determine what is in the best interest of Union or MS law and might face penalties encompassed in the GDPR for disclosing such information. It would however overall, not be a feasible situation and the provider might find itself in a situation where it must choose which obligation to break. If there is not an agreement between the countries where the service provider is located, the service provider do not have legal recourse to quash an order, even if the order might target a non–US person.

One reasons why the Cloud Act shifts jurisdictional focus, to the nationality and residence of the user is to allow foreign governments to respond to the extraterritoriality of the warrant. A service provider may notify a qualifying foreign government of the existence of a warrant or legal process,[170] a prerequisite is that the nationality and residency of the target is known. The notifying mechanism might act as a tool for the qualifying foreign government to object to the information being release about its citizen, thus respecting the principle of sovereignty, but it is only of practical use when the nationality of the user is known. The nationality of the target in the Microsoft Ireland not disclosed, or not known. The jurisdictional basis in the case was the connection of the crime, the consequences of the crime and the psychical location where the FBI would be given the requested information, which would occur in the US. The practical threshold of this mechanism is therefore questionable how effective its execution would be, and to what extent it would be used.

6.3 Bilateral agreements under the Cloud Act and the GDPR

The novelty of the Cloud Act lies in its second part which enables agreements (Cloud Act Agreements; CAA) based on reciprocal principle. The result is that any restrictions imposed on American companies to not share certain stored data with foreign governments are lifted.[171] Foreign states must lift similar prohibitions to allow streamlining of datatransfers.[172] The first agreement to be concluded is between the US and the UK

Orders to obtain information are issued under each country's domestic legal system and sent directly to the service provider. It sets out requirements the orders need to fulfil, and it aims to

[170] Cloud Act section 103(b)

[171] Under the SCA, companies can only share non-content data such as time stamp or the existence of data.

[172] Ben Barnett and others, 'Forecasting the Impact of the New US CLOUD Act' (2018) Dechert LLP.

resolve the third finding of US Congress by clarifying the necessary procedural steps and what needs to be fulfilled for a warrant to have bearing. Additionally, it provides procedural steps for a service provider to challenge such request from a US legal authority to hand over material, however the prerequisites are limited and strict.[173] Service providers must satisfy three criteria in order oppose the warrant within fourteen days of the request being issued: 1) the data concerns a non–US person residing outside the US and 2) if the entity would create a material risk of breaching the law 3) of a qualifying foreign government.[174] It further includes a number of facts that courts must consider when balancing the facts of the case[175] but it does not explicitly include the interest of the target, and does not mention the targeted persons' right to privacy.
The procedural and substantive safeguards – also described as 'target limitation' –specifies permittable targets whose data are sharable. Large scale collection of data is not permitted, and either government cannot intentionally intercept data that is not a national. The foreign state may however target its nationals US territory that are unlawfully residing in the US. Qualified foreign governments can only request data of non–US citizens located outside the US and are prohibited from indirectly or directly target US citizens and residents (US persons).[176] If the qualifying state requests information of a US person it must adhere to MLAT processes.[177] The foreign government cannot seek the information of its own nationals if it risks targeting a US person and, it works two ways. US authorities cannot unintentionally or intentionally target a non–US person. This only applies when there is a CAA in force, which means that US might target EU persons despite infringing upon state sovereignty.

If the EU entered into an agreement with US under the Cloud Act, it would enable law enforcement to access stored data regarding EU persons in a timelier manner than relying on MLAT. The protections afforded under the Act are negotiable, and the EU and the US have announced negotiations are ongoing.[178] There are challenges in these negotiations and what result they might bring which are outside the scope of the thesis, but it is worth mentioning it is in process.

[173] CLOUD Act s 102 (4)– (5).
[174] Cloud Act 2703(h)(2)(A).
[175] Ibid 103(b).
[176] 130Ibid (codified at 18 USC. s 2523(b) (4) (A)–(B).
[177] Jennifer Daskal, 'Unpacking the CLOUD Act' (2019) eruvim 220
[178] Recommendation for a Council decision authorizing the opening of negotiations in view of an agreement between the EU and the USA on cross-border access to electronic evidence for judicial cooperation in criminal matters, COM/2019/70 final, Brussels, 5 February 2019.

7. Conclusion

An order issued under domestic law cannot be transferred under Article 48 GDPR. Article 49(1)(d) may however trigger applicability and for reasons stated below, I argue that a transfer may proceed.

Initially it might seem like the EDPB, and the Commission in the Microsoft case have different interpretations of Article(1)(d), but essentially, they reach similar conclusion. In each their own way, a transfer based on American law is recognised. From the Commission standpoint, any crime that are enumerated in Article 83 TFEU have legal bearing, and from the EDPB standpoint it is merely not enough. What might initially seem like a high threshold for a transfer to have bearing, is not really in the situation in the present situation. The EDPB argues that the best interest must be in both the nation issuing the warrant *and*, in the Union, or a MS. An indicating factor of such might be an international agreement such as a Convention. In the case of an issue under the Cloud Act, the Budapest Convention on Cybercrime may act as such indicator. Both the Union and the US are party to it. An order under the Cloud Act would therefore, not per se infringe on state sovereignty. Even if a foreign court not familiar with the EU legal system would apply either the EDPB or the Commission, it would produce the same result but through different ways.

A service provider would not *per se* violate a Cloud Act order by notifying a qualifying government; an agreement under the Cloud Act must exists between the US and the qualifying foreign government. A transfer can however not be used to the point it can be considered the rule for Cloud Act transfers. The extent of requests is not known or not made public, but it would be an interesting approach to further study.

However, the question to be asked is whether US law permits EU persons to challenge such an order, and if the lack of redress is compatible with Article 47 of the Charter. Since a transfer concerns the right to dataprotection and the right to privacy, it must be read in the light of the Charter. There will be no argument as to the question if such order would infringe on Article 7 and 8 of the Charter, but rather to highlight it might violate Article 47 of the Charter. Albeit the Cloud Act set out 'target limitation' that echoes the principle in the GDPR of necessity, the possibility for an individual to challenge an order is not there and because an individual cannot challenge an order, it cannot be argued that the safeguards ensured by Article 47 are upheld. It additionally does not seem compatible with Article 47 that the limited possibility for a service provider to challenge an order. It can be difficult to argue that it can only be challenged if there is an international agreement linked to the US.

A service provider must stop any transfers occurring if the dataprotection afforded under Union law is undermined when the data leaves the Union. The Cloud Act does not improve the disparities the Court found lacking in the Schrems II case. A practical issue is the option of service providers to challenge an order. If they were to transfer data regarding an EU person, it would violate the GDPR, and the provider may be subject to its high penalties so the question is how thoroughly a service provider might check the nationality of its user when it is faced with a warrant. Since service providers do not generally verify or collect such information, and it might be missed by the US court, what are the consequences of transfers than concern EU persons?

A cumbersome process combined with the strict two-week time limit to determine the nationality and residency of the subject might alone be a time-consuming burden. Further, the state responsible for the datasubjects is not necessarily given an option if it wants to aid the US or not to transfer data. The consequence of such action, in the event an EU person is unknowingly target of an order, and its state is not notified about such order, might constitute an infringement on state sovereignty. The service provider might have contractual obligations to others two other private entities where the service provider might find itself in a situation where it is best to choose which countries law to comply with the law with the highest penalty.

7.1 The Cloud Act tests and Article 47

The legal tests applied under the Act aims to limit transfers by requiring law enforcement to demonstrate there is reason to believe the person is involved in crimes. The Act does however not necessarily take the citizenship of the person into account if it is not known. As seen in the Microsoft example, the nationality of the target was not known, but it was concluded that the location of the crime took place in the US, and therefore the Court ought to compel Microsoft to hand over the data. Since the case did not go to merit, the reasoning of the Court remains unclear.

The target limitation under the Act aims to ensure to not infringe on the sovereignty of other states, but it does at the same time not require the foreign state to necessarily be informed of requests of information about its citizens, and it does not *require* either service providers or US law enforcement to notify the authorities but are not either prevented too do so. To properly respect state sovereignty, it should be made a requirement to notify the authorities of the foreign state concerned so the foreign state have the option to either accept or deny cooperating with the US authorities, or, to take any other action it finds appropriate.

To the point that it is only possible to challenge a court order if there is an existing agreement under the Cloud Act cannot be argued that be in accordance with Article 47 of the Charter. The fact that an individual must rely on a service provider to challenge such orders are a further testament to the incompliance with Article 47, as it is not reasonable due to its status as a fundamental right.

Table of Authorities

Jamie Bartlett, ‘The People Vs Tech: How the Internet is killing democracy (and how to save it)’ (Edbury digital 2018)
Ian Dobison, Francis Johns, ’Qualitative Legal Research’ *in* Mike McConville, Wing Hong Chui (eds.) Research Methods for Law (Edinburgh University Press 2007)
IT Governance privacy team, EU General Data Protection Regulation: An Implementation and compliance guide (4th edn, IT Governance Publishing 2020)
Christopher Kuner, Transborder Data Flows and Data Privacy Law (Oxford University Press 2013)

Journal Articles

Samuel D. Warren, Louis D. Brandeis, ’The Right to Privacy’ (1890) Harvard Law Review Vol. 4 No. 5
Paul M. Schwartz
, ‘Privacy and Democracy in Cyberspace’ (2000) 52 Vand. L. Rev. 1609
Jennifer Daskal, ’The Un-Territoriality of Data’ (2015) The Yale Law Journal 125:326
Jim Isaak, Mina J. Hanna, ’User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection’ (2018) IEEE Computer Society
Paul M Schwartz, 'Legal Access to the Global Cloud' (2018) 118 Columbia Law Review 1681
Els De Busser, ‘The Digital Unfitness of Mutual Legal Assistance’ (2017) Security and Human Rights 28 161
Winston Maxwell, Mark W Brennan and Arpan A Sura, ‘Demystifying the US CLOUD Act: Assessing the Law’s Compatibility with International Norms and the GDPR’ (Hogan Lovells January 2019)
Klaus–Dieter Borchardt, ’The ABC of EU Law’ (2017) Publication’s office of the European Union 91
Marcin Rojszzack, ‘CLOUD act agreements from a EU perspective’ (2020) Computer law & Security Review 105442
Johnathan D Jordan, ‘Out of “Control” Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed By a Foreign Parent?’ (2016) 68 Baylor Law Review.
Haleform H. Abraha, ‘Regulating law enforcement access to electronic evidence across borders: the United States approach’ (2020) Information & Communications Technology Law, 29/3 333
Jennifer Daskal, ‘Unpacking the CLOUD Act’ (2019) eruvim 220
Ben Barnett and others, ‘Forecasting the Impact of the New US CLOUD Act’ (2018) Dechert LLP

Reports

Europol, ‘A corrupting influence: The infiltration and undermining of Europe’s economy and society by organized crime’ EU Socta 2021 – Serious and Organized Crime Threat Assessment
US Department of Justice, ‘Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act’ (White Paper, April 2019)

Web material

Judith Duportail, ‘I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets’ (26 September 2017) <https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold> accessed 10 May 2021
Facebook terms of use, accessed 16 April 2021

Sam Levin, ‘Is Facebook a publisher? In public it says no, but in court it says yes’ (3 July 2018) <https://www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit> accessed 10 May 2021.
Alex Hern, ‘Cambridge Analytica: how did it turn clicks into votes’ (6 May 2018) <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie> accessed 10 May 2021.
Rikard. Lindholm, ‘Project Alamo’s Data-driven Ads on Facebook won Trump the Election’ (Semantiko 19 February 2017) <https://semantiko.com/project-alamo-trump-facebook-ads> accessed 16 April 2021.
Devjyot Ghoshal, ‘Mapped: The breathtaking global reach of Cambridge Analytica’s parent company’ (28 March 2018) <https://qz.com/1239762/cambridge-analytica-scandal-all-the-countries-where-scl-elections-claims-to-have-worked/> accessed 10 May 2021
Clint Boulton, ‘NSA's Prism Could Cost IT Service Market $180 Billion’ Wall Street Journal (16 August 2013) <https://blogs.wsj.com/cio/2013/08/16/nsas-prism-could-cost-it-service-market-180-billion/> accessed 10 May 2021
Peter Sayer, ‘For Germany’s Cloud Providers, It’s Location, Location, Location’ (14 March 2016) Network World

Miscellaneous

Letter from Assistant Att’y Gen. Peter Kadzik to Vice-President Joseph R. Biden, President, United States Senate (July 15, 2016)
DPBD, ‘Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)’ 12 November 2019
Peter Mell, Timothy Grance, ‘The NIST definition of Cloud Computing: Recommendations of the National of Standards and Technology’ (2011) NIST Special Publication 800-145
EDPB, ‘Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electric evidence’ (2018) < https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en> accessed 23 May 2021.
EDPB, ‘Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/673’ (2018)