College of Europe
Collège d'Europe
Brugge
Natolin

College of Europe

Bruges Campus

Department of European Legal Studies

One Cloud in the Sky and Conflicting Laws on the Ground

Regulating Law Enforcement Access to E-Evidence in Cloud Computing in the European Union and the United States

Mayer Brown Award

29th of June of 2018

Supervised by: Professor **Claire BURY**
Presented by: **Roberto YUNQUERA SEHWANI**

Statutory Declaration

I hereby declare that the thesis has been written by myself without any external unauthorized help, that it has been neither presented to any institution for evaluation nor previously published in its entirety or in parts. Any parts, words or ideas, of the thesis, however limited, and including tables, graphs, maps, etc., which are quoted from or based on other sources have been acknowledged as such without exception.

Word Count: 14,708

Excluding the cover page, the table of contents, the keywords, the declaration of honor, the abstract, the annexes and the bibliography.

Abstract

The widespread use of cloud computing has led to increased difficulties for law enforcement agencies in the context of criminal investigations. In order to access personal data which may constitute criminal evidence, it is no longer sufficient to seize the user's devices (i.e. desktops, laptops or mobile phones). The most relevant data for criminal investigations, such as e-mails, photos or documents, are now typically stored in a data center operated by a cloud service provider. In this context, the paper offers an overview of the legal instruments which allow law enforcement bodies in the European Union and in the United States to seek disclosure of cloud data. Given that the cloud may be accessed from any device which has a connection to the Internet, regardless of its physical location, it is likely that the data of a user is stored abroad. Consequently, conflicts of laws may become commonplace, for example, when the disclosure of cloud data is simultaneously prescribed by the laws of one state and prohibited by the laws of another state.

This paper starts by analyzing two central cases in which national courts have had to decide whether or not to claim jurisdiction over cloud data, namely *Microsoft Ireland*, before the United States Court of Appeals, and *Yahoo! Belgium*, before the Belgian Supreme Court. Once the factual context is laid out, the paper summarizes the theoretical challenges to conceptualize law enforcement in the cloud economy. Different theories are thus contrasted in order to defend that, despite the existence of potential conflicts of laws, states should nevertheless take appropriate steps to assert jurisdiction and enforce criminal law.

The fact that states should enforce jurisdiction over cloud data is taken as a standpoint from which the question of the solution of existing conflicts of laws is addressed. By comparing different models, such as Mutual Legal Assistance Treaties, principles of international comity or the 2001 Budapest Convention of Cybercrime, the paper concludes that further regulatory intervention is needed to successfully tackle the problem. Finally, the recent examples of the US CLOUD Act and the European Commission e-Evidence Proposal are also considered. After critically analyzing the content of each set of rules, the paper concludes that international agreements are needed in order to prevent and solve conflicts of laws which, in turn, would facilitate law enforcement in the cloud economy.

Keywords

Area of Freedom, Security and Justice
Budapest Convention on Cybercrime
Cloud Computing
Criminal investigations
Commission e-Evidence Proposal
Conflict of Laws
Cybercrime
Electronic Evidence
International Comity
Judicial Cooperation
Law Enforcement
Microsoft Ireland case
Mutual Legal Assistance Treaties (MLAT)
Transatlantic Data Flows
US CLOUD Act

List of Abbreviations

CEPS: Centre for European Policy Studies.

CFREU: Charter of Fundamental Rights of the European Union.

CLOUD Act: Clarifying Lawful Overseas Use of Data Act (United States).

CSP: Cloud Service Provider.

ECPA: Electronic Communications Privacy Act.

EPO: European Preservation Order and European Production Order.

GDPR: General Data Protection Regulation – Regulation (EU) 2016/679.

LEA: Law Enforcement Agency.

TEU: Treaty on European Union.

TFEU: Treaty on the Functioning of the European Union.

USC: United States Code.[1]

WP29: Article 29 Data Protection Working Party, established by Directive 95/46/EC.

[1] United States Acts and Statutes will be cited throughout this paper as titles and sections of the United States Code, as established by the Cornell Legal Information Institute, https://www.law.cornell.edu/citation/2-300

Table of Contents

"It is very difficult to do business if you have to wake up every day and say: okay, whose laws do I follow? We have many countries and many laws and just one Internet."

Heather KILLEN
Former Senior Vice President of International Operations
Yahoo! Inc.

I. Introduction

Clouds have arrived. And they are here to stay. Despite that the average Internet user does not fully understand how the cloud operates, an important number of services we consume online are now based on clouds.[2] Their popularity stems from the advantages they provide to users. Unlike traditional computer technologies, cloud computing offers needs-based processing power and storage space, accessible from any device connected to the Internet, at very competitive prices. The apparent technical ubiquity in which clouds are based, stands in stark contrast with the legal reality. As quoted in the opening phrase, data is in fact constantly crossing national borders. Given the territorial nature of state jurisdiction, the hyperactive data flows generated by cloud computing will typically lead to conflicts of laws.

One of the most typical scenarios in which conflicts of laws arise relates to the access to data which may constitute electronic evidence, or "e-Evidence," by Law Enforcement Agencies (hereinafter, "LEAs") in the context of criminal investigations. Outside the cloud environment, data is always stored in a device under the control of users, i.e. desktops, laptops or mobile phones. To seek disclosure of relevant data, police officers may simply request a court order to seize the users' devices. Where clouds are involved, however, user data is stored in the data centers operated by the Cloud Service Provider (hereinafter, "CSP"). In the cloud economy, even if all the elements of an investigation (i.e. relevant facts, victim and accused) are present in the same state, it is still likely that the data is stored in a data center located in a different state.

In these cases, the domestic laws to which LEAs are subject (which are usually the *lex loci delicti commissi*) tend to require disclosure of the relevant data in the context of the criminal investigation. But it is likely that the act of disclosure is simultaneously governed by the laws of the state in which the data is stored (*lex loci rei sitae*) or in which the CSP is established (*lex personalis*). If either the *lex loci rei sitae* or the *lex personalis* prohibit disclosure to the authorities of the state conducting the criminal investigation, the CSP will find itself in the position of deciding which laws to follow and which laws to breach.

[2] D. ANDREWS, J. NEWMAN, "Personal Jurisdiction and Choice of Law," (2013) 73 *Maryland Law Review*, p.324. Hereinafter, "ANDREWS and NEWMAN."

Given the contradicting legal obligations, compliance with both legal systems simultaneously is impossible.[3] These conflicts of laws, in which two or more legal systems govern the same act of disclosure are particularly complex. A dangerous solution involves data localization rules, under which data of domestic persons must be stored domestically.[4] These requirements stifle innovation and prevent the economic efficiencies brought by the cloud economy.[5]

The United States Court of Appeals had the opportunity to address these issues in the *Microsoft Ireland* case on 14 July 2016.[6] The judgment was later brought to the US Supreme Court, with the hearing taking place on 27 February 2018.[7] While scholars and privacy advocates awaited this potentially groundbreaking Supreme Court judgment, the US Congress surprisingly decided to solve the case by law on 23 March 2018. As part of the annual budget law,[8] Congress adopted the Clarifying Lawful Overseas Use of Data Act (hereinafter, "CLOUD Act").[9] This law explicitly allows US courts to order, in some cases, disclosure of data controlled by American companies regardless of where the data is located.[10] After the signing of the CLOUD Act into law, the Supreme Court decided to vacate and dismiss the case as 'moot'.[11]

This development triggered reactions in other regions of the planet. The European Commission was in fact preparing a legislative proposal after the Council had issued guidelines to orient future EU action already on 30 March 2016.[12] The Commission, seizing the opportunity, issued a Proposal on 17 April 2018 to adopt a Regulation establishing the "European Preservation Order" and the "European Production Order"

---

[3] *See* A. WOODS, "Against Data Exceptionalism", (2016) 68 *Stanford Law Review*, p.735. Hereinafter, "WOODS 2016."
[4] N. GULYAEVA, M. SEDYKH, "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content come Into Effect," 18 July 2014, *Hogan Lovells Chronicle of Data Protection*. Accessed on 21 April 2018 on https://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/
[5] *See* WOODS 2016, *supra* note 3, p.751.
[6] Court of Appeals, Judgment of 14 July 2016, *Microsoft Corporation v United States*, 2nd Circuit, 14-2985. Hereinafter, "*Microsoft Ireland*."
[7] Full transcripts available on https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf
[8] Consolidated Appropriations Act, 23 March 2018, Public Law No.115-141 (2018).
[9] Consolidated Appropriations Act, 23 March 2018, Public Law No.115-141 (2018), Division V. Hereinafter, "CLOUD Act."
[10] 18 USC §2713.
[11] Supreme Court, Order of 17 April 2018, *United States v Microsoft Corporation*, No. 17-2.
[12] Council Conclusions of 30 May 2016, on Improving Criminal Justice in Cyberspace, ST 9579/16 INIT.

(hereinafter, the "e-Evidence Regulation")[13] together with a Directive which requires CSPs to appoint representatives in one of the EU Member States (hereinafter, the "e-Evidence Directive").[14]

Taking into account the high speed of legislative developments in the field, this paper analyzes the extent to which the proposed solutions constitute an adequate balance between the interest of obtaining e-Evidence, on the one hand, and the objective of minimizing conflicts of laws and protecting fundamental rights, on the other hand. Although the term e-Evidence will be often used in the following paragraphs, this study is rather concerned about access to "data with criminal relevance," given that "evidence" under criminal law refers to information which has already been cross-examined in court.[15]

Despite the relative wealth of scholarship in the topic, particularly American, this paper aims to complement existing research by offering a perspective under European Union law in light of the recent developments proposed by the European Commission. The following chapters will, thus, emphasize the privacy concerns raised by the CLOUD Act and the e-Evidence package, with a view to recommend additional reforms which could ensure effectiveness of law enforcement without undermining privacy and data protection rights.

To achieve these objectives, Chapter II will focus on the academic debate surrounding state jurisdiction in the cloud environment. The overview of the main judicial disputes involving cloud data in the US and the EU will offer the factual framework to analyze whether states can and should legitimately assert jurisdiction over cloud data stored within their borders. This overview also contributes to highlight the rise of conflicts of laws between states when asserting jurisdiction over clouds. Chapter III will then analyze the currently applicable rules, including international law instruments as well as general principles of law, to assess whether they provide national courts with adequate tools to successfully solve existing conflicts of laws. Finally, Chapter IV will condense the critical

---

[13] European Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters [2018] COM(2018)225 final. Hereinafter, "e-Evidence Regulation."
[14] European Commission Proposal for a Directive laying down rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, [2018] COM(2018)226 final. Hereinafter "e-Evidence Directive."
[15] *See* Joe MCNAMEE, "Towards a European Production Order?", 31 January 2018, CPDP Conferences. Accessed on 25 April 2018 on https://www.youtube.com/watch?v=8z6Cx7qLLHg

evaluation of the US CLOUD Act and the EU e-Evidence Proposal, together with the assessment of the future steps that the EU should take.

II. Asserting Jurisdiction over Data

Clouds are based on the pooling of computing and storage capacity by different devices.[16] When a cloud service is provided, user data is stored in the CSP's data centers, rather than in the devices owned by users.[17] The capacity provided to the user is pooled by the CSP depending on the particular demand at any given moment,[18] which turns clouds into highly elastic networks of computing capabilities.[19] Following the definition laid down by the US National Institute for Standards and Technology, clouds provide a sense of "location independence" insofar as the customer "generally has no control or knowledge over the exact location of the provided resources."[20] Users are unaware of the location of the provided capabilities, given that they are granted access from any device over the Internet. This definition of cloud computing encompasses cloud-based e-mail services, in which messages are stored in the service provider's data centers.

As noted in the Introduction, these attributes of cloud computing lead to situations in which two or more states claim jurisdiction over the same data or, even, impose contradicting obligations regarding the same data. Hence, this chapter dives into the legal status of the cloud and the extent to which it is legitimate that several states claim jurisdiction over cloud data. Given the complexity of the issues tackled in the paper, the chapter will start by developing two cases in which cloud data has generated challenges for the assertion of state jurisdiction. Indeed, Section 2.1. analyzes the case of *Microsoft Ireland* in the United States, while Section 2.2. turns to the latest *Yahoo! Belgium* case, before the Belgian Supreme Court, to develop the challenges faced by law enforcement when asserting jurisdiction over clouds. These two cases will be quoted as examples in following chapters. Finally, Section 2.3. places the conclusions inferred from the case law within the theoretical debate concerning the legitimacy of state jurisdiction over the Internet. This last section shows that the issues tackled in this paper are not only relevant for the specific case of e-Evidence, but also to understand the regulation of other online-based fields such as algorithms or the Internet of Things.

---

[16] J. KLEIJSSEN, P. PERRI, "Cybercrime, Evidence and Territoriality: Issues and Options," (2016) 47 *Netherlands Yearbook of International Law*, p.159.
[17] National Institute for Standards and Technology, The NIST Definition of Cloud Computing, US Department of Commerce, [2011] 800-145.
[18] *Ibid.*
[19] *Ibid.*
[20] *Ibid.*

2.1. An American Perspective: The *Microsoft Ireland* Case

Extraterritoriality of state power, conflict of laws and protection of privacy were the ingredients of the controversial *Microsoft Ireland* case. The unusual circumstances in which it took place certainly led to a high degree of press coverage. After the US Court of Appeals released its judgment, the case was brought before the US Supreme Court. However, before the Court ruled on the matter, Congress adopted the CLOUD Act, which solved the dispute at issue. Hence, the Supreme Court vacated the judgment and ordered the District Court to dismiss the case as moot.[21]

The case was brought to the Court of Appeals following Microsoft's refusal to comply with a "Search and Seizure Warrant", issued on 4 December 2013. The US Government, in the context of a drug investigation,[22] sought access to *inter alia* the content of e-mails, identification records (IP addresses, telephone numbers, etc.) and address books regarding several web-based e-mail accounts operated by Microsoft Corporation (@msn.com).[23] Microsoft disclosed basic account information and the address books, but refused to grant access to the content of the e-mails on grounds that they were not stored in the United States, but in Microsoft's data center in Dublin.[24] Indeed, under Microsoft's data management policies, content data is migrated to the data center which is closest to the users' state of residence, for efficiency reasons.[25] Consequently, it only retains basic, non-content data, in its US servers.

The warrant was issued under the 1986 Electronic Communications Privacy Act (hereinafter, "ECPA"),[26] specifically under Title II, which is often referred to as Stored Wire Electronic Communications Act. The law prohibits disclosure of content data to third parties unless the appropriate judicial authorizations have been obtained.[27] The types of data which pose a smaller risk to privacy, namely subscriber and transactional data may be

[21] Supreme Court, *United States v Microsoft*, *supra* note 11.
[22] *Microsoft Ireland*, *supra* note 6, p.4.
[23] *Ibid*., p.10.
[24] *Ibid*., p.5.
[25] To reduce "network latency," see *Ibid*., p.8.
[26] Electronic Communications Privacy Act 1986, Public Law No.99-508, 18 USC §2701–2712. Hereinafter, "ECPA."
[27] 18 USC §2703(b).

disclosed following an administrative subpoena, which is not subject to judicial review.[28] Content data is protected by a "Search and Seize Warrant," subject to thorough judicial scrutiny. Court warrants are only issued when a high evidentiary threshold has been met, namely the Fourth Amendment "probable cause" standard.[29] The main question submitted to the US Court of Appeals, therefore, sought to ascertain whether the disclosure of data stored in Dublin by Microsoft's "wholly owned" subsidiary[30] constituted an extraterritorial application of the ECPA.

The US Court of Appeals, agreeing with Microsoft, followed a two-step approach to determine whether the ECPA had been applied to an extraterritorial situation. Firstly, it noted that the ECPA did not explicitly authorize extraterritorial application.[31] Under US common law it is presumed that the silence of a statute indicates that possible extraterritorial effects were rejected by the legislature. Secondly, the Court analyzed whether the warrant requesting data stored abroad was in fact an extraterritorial application of the law.

To decipher whether the warrant served to Microsoft constitutes an extraterritorial application of the ECPA, the Court noted that the 'focus' of the ECPA was the protection of privacy.[32] Contrary to the assertions of the US Government, when focusing on privacy, the relevant conduct targeted by the statute is the access to the data. Even if disclosure of the e-mails by Microsoft would only take place in the US, the company would be "accessing" the data in Ireland. Hence, relying upon a warrant under the ECPA to access data stored in Ireland would amount to an unlawful interpretation of the ECPA due to its extraterritorial effects.[33] The fact that the data could be transferred from Ireland back to the US in seconds was not accepted as a relevant argument.[34] The Court noted that Microsoft's

[28] U.S. Department of Justice, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities. Accessed on 26 April 2018 on https://www.justice.gov/archive/olp/rpt_to_congress.htm
[29] WOODS 2016, *supra* note 3, p.749.
[30] *Microsoft Ireland*, *supra* note 6, p.7.
[31] *Ibid.*, p.21-22.
[32] *Ibid.*, p.32-38.
[33] *Ibid.*, p.39.
[34] *Ibid.*, p.20.

employees, even if based in the US, would necessarily "interact with the Dublin data center in order to retrieve the information" [35] and *bring it into* the US.

Therefore, the Court of Appeals in *Microsoft Ireland* prevented the disclosure of data by Microsoft under an ECPA warrant. However, Professor Kerr interpreted the relevance of the Court of Appeals' judgment in an uncommon yet thought-provoking manner. Professor Kerr argued that the Court of Appeals simply declared the ECPA inapplicable to seek access to data stored abroad. But the ECPA is a privacy statute. It orders the US Government to rely upon special instruments, such as court warrants, to obtain disclosure of electronic communications data. In the absence of the ECPA's special provisions, the US Government could rely upon administrative subpoenas, which are typically used to obtain physical documents, to access electronic communications data. If the ECPA as a whole does not govern the access of data stored in Dublin, the US Government could, thus, issue an administrative subpoena, with no judicial oversight, to order disclosure of e-mails. Privacy rights enshrined by the ECPA would not oppose this strategy.[36]

The previous example shows that the US Government, even after the ruling of the Court of Appeals in the *Microsoft Ireland* case, has alternatives to seek access to cloud data. The recently enacted CLOUD Act hints in the same direction, by explicitly granting extraterritorial reach to ECPA warrants. The problem arises when taking into consideration that disclosure ordered by the US Government may breach the rights enshrined by other jurisdictions. As stated in the European Commission's amicus curiae brief before the US Supreme Court, EU law is fully applicable to govern processing of data stored by Microsoft in Ireland.[37] Hence, data transfers to the US should only be completed by Microsoft when provided for by EU law. The first question which will be addressed in the final section of this chapter concerns the extent to which both the EU and the US have a legitimate interest in regulating Microsoft's data. The possible solutions to this conflict of laws will be analyzed in following chapters.

---

[35] *Ibid*., p.40.
[36] *See* O. KERR, "What legal protections apply to e-mail stored outside the US?", 7 July 2014, *The Washington Post*. Accessed on 22 April 2018 on https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/?noredirect=on&utm_term=.fa87a2e88ea6
[37] European Commission, Amicus Curiae for the Supreme Court, *United States v Microsoft*, No. 17-2, p.3.

2.2. The Challenges in Europe: The Yahoo! Belgian saga

On the other side of the Atlantic, the situation was not much different. In Belgium, the *Cour de Cassation*[38] was requested in 2015 to rule over a case concerning data held by Yahoo! Inc. The Belgian public prosecutor issued an order, on the basis of article 46 bis of the *Code d'Instruction Criminelle*,[39] to seek access to the data. This provision determines that public prosecutors are entitled to request the cooperation of electronic communications service providers to obtain criminal evidence. The Court was requested to ascertain whether these rules were applicable to service providers which were not established in Belgium. In this case, the Court noted that the cooperation obligation stated in article 46 bis is "committed at the place where the requested information must be received."[40] Consequently, disclosure orders served to a company which is not established in Belgium does not amount to an extraterritorial application of Belgian law.

The 2015 judgment must be read as strengthening settled case law concerning data held by Yahoo! Inc. Indeed, past cases suggest that the Court only rarely questioned that orders issued by Belgian public prosecutors could have extraterritorial effects. In 2011, Yahoo! Inc. claimed that it was not subject to article 46 bis insofar as it was not a provider of electronic communications services. The Court rejected this argument, on the basis that electronic communication services encompassed services which consist "wholly *or mainly* in the conveyance of signals through electronic communications networks"[41] (emphasis added).

By using the criterion of the place of disclosure, the *Cour de Cassation* opens the door to apply Belgian law to data located abroad. If the relevant connecting factor is not the place where the data must be accessed, but the place where the data must be disclosed, the duty of cooperation with Belgian public prosecutors has a clear extraterritorial reach. The Belgian Court, therefore, upholds a similar argument than that of the US Government in the *Microsoft Ireland* case. This situation leads to conflicts of laws whenever the laws of another state prohibit the disclosure of data on data protection grounds.

---

[38] Belgian Supreme Civil Court.
[39] Code d'Instruction Criminelle (Belgian Code of Criminal Procedure), 17 November 1808, as amended by the Loi modifiant l'article 46bis du Code d'instruction criminelle, 23 January 2007, article 46 bis.
[40] Cour de Cassation, Judgment of 1 December 2015, *Procureur-Général c Yahoo! Inc.*, P.13.2082.N, p.7.
[41] Cour de Cassation, Judgment of 18 January 2011, *Procureur-Général c Yahoo! Inc*., P.10.1347.N, p.4.

2.3. Territoriality, Data and Jurisdiction

In the wake of the *Microsoft Ireland* and *Yahoo! Belgium* cases, many scholars have revived the argument that states are simply ill-equipped to regulate the cloud economy. Given the borderless nature of clouds, territory-based laws cannot properly define rights and obligations of cloud users and CSPs.[42] To delve into this debate, the concept of jurisdiction should be further developed. State jurisdiction is typically defined as "the reach of the law of one state over acts and individuals."[43]As Professor Woods indicated, jurisdiction can be divided in two elements: prescriptive jurisdiction and enforcement jurisdiction. The former broadly denotes the capacity of a state to prescribe or regulate a specific behavior. Conversely, the latter involves the implementation of rules over a specific behavior, in order to change it.[44]

It is the notion of prescriptive jurisdiction which has led scholars to reject state jurisdiction over cloud data altogether. Their position is based on two possible grounds. Either a) The global Internet should not be regulated by territorial state jurisdictions, or b) States do not have a legitimate claim over cloud data simply because it is stored within their borders. The following paragraphs will now address these debates separately.

2.3.1. State Jurisdiction over the Global Internet

Already in 1996, Johnson and Post were seen as some of the strongest advocates of the notion that states could not –and should not– "reach over" online behavior. In their opinion, online behavior "exists, in effect, everywhere, nowhere in particular, and only in the Net."[45] Cyberspace concerns things, i.e. messages or databases, which are not separated by physical boundaries.[46] This particular analysis of the online sphere brings them to the

[42] *See* D. JOHNSON, D. POST, "Law and Borders: The Rise of Law in Cyberspace", (1996) 48 *Stanford Law Review*, p.1379; or ANDREWS and NEWMAN, *supra* note 2, p.365.
[43] S. CARRERA, G. GONZÁLEZ FUSTER, E. GUILD, V. MITSILEGAS, [2015] "Access to Electronic Data by Third-Country Law Enforcement Authorities," Centre for European Policy Studies, p.57. Hereinafter, "CEPS."
[44] WOODS 2016, *supra* note 3, pp.765 and 769-770.
[45] JOHNSON, POST, *supra* note 42, p.1375.
[46] *Ibid*., p.1376.

conclusion that "no geographically located set of constituents has a more legitimate claim to regulate online activities"[47]

A few years after Johnson and Post published their controversial article, Goldsmith offered a strong set of counter-arguments. In his view, legal systems, taken as a whole, have multiple instruments at their disposal to claim and enforce jurisdiction, even when the physical location of the asset in question is unclear. To compare these two perspectives, the arguments regarding effectiveness of jurisdiction will be considered in the first place, followed by the arguments concerning the legitimacy of jurisdiction enforcement.

Firstly, Johnson and Post argue that asserting jurisdiction over "electronic information across physical borders" should be rejected given that the enforcement of such jurisdiction "is likely to prove futile."[48] If ever a state desired to prohibit a specific behavior online, the concerned user could simply "reconfigure his connection so as to appear to reside in a location outside the particular state."[49] It must be acknowledged that, in principle, a state may only enforce its jurisdiction against "persons or entities with a presence or assets within its territory."[50] However, jurisdiction over cloud data can easily be enforced if a state, for instance, targets local end-users who participate in an illegal transaction or impose obligations on parties that facilitate the transaction, such as Internet service providers or financial institutions with a local presence.[51] As Woods argues, the key element to determine whether enforcement is possible "is not where the data is stored –or how mobile, interchangeable, or tangible it is– but rather whether the Court can assert personal jurisdiction over a defendant with the ability to access that data."[52]

Secondly, Johnson and Post claim that state jurisdiction on the Internet should be rejected as illegitimate, even if its enforcement was technically possible. They note that in the physical world, individuals are made aware that they will be subject to a different jurisdiction whenever they cross a border. On the contrary, "in cyberspace physical borders no longer function as signposts informing individuals of the obligations assumed by

[47] *Ibid.*
[48] *Ibid*., p.1372.
[49] *Ibid*., p.1374.
[50] WOODS 2016, *supra* note 3, p.770.
[51] J. GOLDSMITH, "Against Cyberanarchy", Occasional Papers, (1999) 40 *Chicago Law School Publications*, p.19.
[52] WOODS 2016, *supra* note 3, p.771.

entering into a new, legally significant place."[53] While it must be accepted that the users may not be aware of which laws will be applicable to a specific online behavior, "no nation has yet imposed liability on a content provider for unforeseen effects in an unknown jurisdiction."[54] States will only exercise their jurisdiction whenever there is a reasonable connection with their territory to do so. Consequently, the mere fact that the targeted behavior took place online should not stand as an impediment to assert jurisdiction.

The reasoning that seems to better capture the reality of cloud computing, is that of Professors Goldsmith and Woods. In this regard, data "is not conceptually novel enough,"[55] to fundamentally challenge the concept of states' territory-based prescriptive jurisdiction. Data, in Woods' view "has physical and intangible features, both of which provide helpful precedent for states seeking to assert jurisdiction over [it]."[56] The reasons which support the previous statement will, in the following paragraphs, also lead to the conclusion that the state in which cloud data is located has a legitimate claim over such data.

2.3.2. Regulating Cloud Data

If a crime has been committed in the territory of a state, it can be concluded that local judges may assert jurisdiction over the persons and goods which explain the facts, including data.[57] The fact that the requested data is located outside state borders does not legitimately derogate from the interest of a state in prosecuting crime. However, it has been argued that states do not have a legitimate claim over data which is stored within their borders, on grounds that all the persons to which it relates, or the behavior which it reflects, happened in a different state. Consequently, the assertion of state jurisdiction over data has been criticized whenever the basis for such jurisdiction simply relates to the fact that it was stored in its territory.

Microsoft's data management policies, as explained to the Court of Appeals in the *Microsoft Ireland* case, serve to illustrate this point. In effect, when an e-mail account is

---

[53] JOHNSON, POST, *supra* note 42, p.1375.
[54] GOLDSMITH, *supra* note 51, p.18.
[55] WOODS 2016, *supra* note 3, p.729.
[56] WOODS 2016, *supra* note 3, p.734.
[57] *Ibid*., p.765-766.

created, Microsoft allows users to self-report their residence.[58] With no further review, Microsoft immediately deletes the user's data from its US servers, except for the account and contact information, and migrates it to the data center which is closest to the user's declared residence. This system, which was adopted to facilitate users' access to their data, is indeed subject to abuse. In order to increase the difficulty of US LEAs to access data relevant to a criminal investigation, an individual may simply report a location outside the US territory. While this situation could trigger a conflict of laws, it is not sufficient to reject the legitimate jurisdiction of both the state in which the crime was committed (*locus delicti commissi*) and the state in which the data is stored (*locus rei sitae*).

There is a legitimate interest in ensuring that a state will not cause harm to another state by ordering disclosure of data stored within its borders. Data is typically subject to regulation to prevent potential harm to citizens' privacy rights. In the case of *Microsoft Ireland*, even if the users of the e-mail accounts were US citizens, residing in the US, who used the accounts to enter into unlawful commercial activities involving narcotic substances in the US, Ireland would still have a legitimate claim to assert its jurisdiction. The sought data constituted personal data processed by an Irish undertaking (i.e. Microsoft Ireland Operations Ltd.). It cannot be denied that the Irish Government has a legitimate interest in regulating the data processing activities of an undertaking established in Ireland, regardless of the origin of the data or the users it concerns.

This conclusion is further reinforced when placing it in the broader context of EU law. In the Union's legal system privacy and data protection are considered fundamental rights, as recognized under articles 7 and 8 of the EU Charter of Fundamental Rights (hereinafter, "CFREU")[59]. In this regard, fundamental rights under EU law are not granted solely to EU citizens or to EU residents but apply to "everyone."[60] EU data protection law stems from the aforementioned fundamental rights, through statutes which have been enacted as specification and interpretation of these rights.

---

[58] *Microsoft Ireland*, *supra* note 6, concurring opinion of E. LYNCH, p.15.
[59] Charter of Fundamental Rights of the European Union, 12 December 2012, O.J. 364/01. Hereinafter, "CFREU."
[60] CEPS, *supra* note 43, p.29.

The General Data Protection Regulation (hereinafter, "GDPR"),[61] as the backbone of EU data protection law, grants specific rights to individuals whose personal data is subject to processing activities by undertakings established in the EU or who carry out specific commercial activities in the EU.[62] In addition, the GDPR also imposes specific obligations on undertakings established in the EU, which are involved in the processing of personal data. The GDPR indicates that controllers and processors of personal data must adopt "appropriate technical and organizational measures to ensure a level of security"[63] appropriate for the type of personal data which is processed. These entities, in addition, must appoint a Data Protection Officer in order to monitor compliance with EU data protection law[64] and cooperate with the national authorities competent in this field. In the event that a personal data breach took place, the controller and the processor must share information about the breach, in order to notify the competent authorities and the user affected by the breach.[65]

The Court of Justice already showed its willingness to minimize any risk to privacy and data protection, given their nature of fundamental rights under EU law. In Digital Rights Ireland, the Court found an infringement of the fundamental rights to privacy an data protection, among other reasons, because it "[allowed] the competent national authorities to access [personal] data."[66] The Court noted that the possibility of accessing personal data, in and of itself, "derogates from the system of protection of the right to privacy."[67] Therefore, "to establish the existence of an interference with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way."[68] It can, thus, be inferred from this case that foreign LEA access to data stored in the EU will be seen by the Court as an infringement of EU fundamental rights. While infringements may be justified, provided that they do not affect the essence of the rights in question, the

[61] Regulation (EU) 2016/679 of 27 April 2016, 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, [2016] O.J. L119/1. Hereinafter, "GDPR."
[62] *Ibid*., article 3.
[63] *Ibid*., article 32.
[64] *Ibid*., articles 37 and following.
[65] *Ibid*., articles 33-34.
[66] Judgment of 8 April 2014, *Digital Rights Ireland v Minister for Communications*, C- 293/12 and C- 594/12, EU:C:2014:238, p.32.
[67] *Ibid*., p.32.
[68] *Ibid*., p.33.

infringements must meet the EU standard of proportionality.[69] In light of these considerations, the EU has a legitimate concern in asserting jurisdiction over data processed by an undertaking established in the EU, regardless of the user to whom they refer or the state in which they are processed.

There is no reason which justifies that a state should not seek to assert jurisdiction over data which is stored within its borders, in order to enforce these rights and obligations, despite that it relates to citizens of other states or is used for criminal purposes there. In this context, questions concerning cloud data will not be solved by rejecting the jurisdiction of one of the interested states, nor by creating a specialized international court which would have exclusive jurisdiction over cloud data. Legal uncertainty and unreasonable distinction between online and offline behavior would be the resulting outcome should any of the previous alternatives be accepted. States should have the capacity to assert and enforce jurisdiction over cloud data whenever it is located within its borders or when it is relevant to investigate crime committed domestically. Hence, if it is legitimate that states enforce jurisdiction over cloud data, the existence of conflicts of laws must be deemed inevitable. The debate should, consequently, focus on possible solutions to conflicts of laws.

[69] *Ibid*., p.45.

III. Addressing Conflicts of Laws: The Regulatory Framework

As has been analyzed in Chapter II above, it is likely that cloud data generates conflicts of laws insofar it is possible that more than one state has a legitimate interest to assert jurisdiction over the same data. Typically, one state will have an interest in investigating criminal activity which happened in its territory; and another state, in assessing whether compliance with an investigative measure may harm domestic fundamental rights. As the US Court of Appeals indicated, "in a world where commercial transactions are international in scope, conflicts are inevitable."[70]

In this context, conflicts of laws or conflicts of jurisdictions may affect the enforcement of domestic law. Legal systems are endowed with a series of instruments and principles which ensure that courts will take "every reasonable precaution" to avoid placing individuals in a situation in which they must comply with two contradicting obligations imposed by two different legal systems. These principles prevent courts from surrendering to the notion that "criminal investigations must be thwarted whenever there is conflict with the interest of other states." [71]

In this broad view, concerns over conflicts of laws may lead to the adoption of different mechanisms. According to the research carried out by the Centre for European Policy Studies (hereinafter, "CEPS"), these mechanisms are classified in two groups: mediated models and unmediated models. Under mediated models, conflicts of laws are solved *ex ante*. Authorities from the two states which claim jurisdiction over the data review the LEA order to ensure that no legal system opposes the disclosure. [72] In this model, no enforcement activity takes place without the assent of the *lex loci rei sitae*. On the contrary, under the unmediated model, conflicts of laws will be solved *ex post*. Indeed, the availability of data through electronic means empowers LEAs to seek disclosure of data without the prior assessment of local authorities.[73] By relying on international comity

[70] Court of Appeals, Judgment of 13 May 1976, *United States v Field*, 5th Circuit, 532 F.2d 404, p.13.
[71] *Ibid.*, p.13.
[72] CEPS, *supra* note 43, p.6.
[73] *Ibid.*

principles, the state issuing the order will unilaterally decide whether or not the disclosure order should be enforced.

To analyze these questions, Section 3.1. addresses the notion of Mutual Legal Assistance Treaties as the archetypical example of legal instruments based on the mediated model to prevent conflicts of laws. Subsequently, the analysis of the unmediated model will be addressed in the two following sections. On the one hand, Section 3.2. focuses on principles of international comity; on the other hand, Section 3.3. includes a thorough analysis of the main body of international law which governs LEA data access, namely the 2001 Council of Europe Convention on Cybercrime.

3.1. The Mediated Model: Mutual Legal Assistance Treaties

After the Court of Appeals ruling in the *Microsoft Ireland* case, many scholars argued that the US Government would have to seek assistance from the Irish Government in order to access the sought data. Judicial cooperation between states is typically regulated in Mutual Legal Assistance Treaties (hereinafter, "MLATs"). MLATs reflect a major departure from the old general principle of law according to which "the courts of no country execute the penal laws of another."[74] Under an MLAT, the authorities of a receiving state (typically, the *locus rei sitae*) will review and execute an order sent by the authorities of an issuing state (typically, the *locus delicti commissi*).

MLATs succeeded in extending the reach of LEAs to enforce jurisdiction over persons or objects which were located in another state. To achieve this objective, MLATs were based on the premise that the authorities of each state shall ensure compliance with their respective legal systems. As the Federation of German Industry noted in its amicus curiae brief for the *Microsoft Ireland* appeal, MLATs are "manifestations of fundamental principles of state sovereignty", namely "that one sovereign nation's officials will not exercise their jurisdiction on a foreign state without consent."[75] By requiring participation of the competent authorities of both states, compliance with both legal systems is ensured

[74] Supreme Court, Judgment of 16 May 1827, *The Antelope*, 25 U.S. 546, p.123.
[75] Bundesverband der Deutschen Industrie, Amicus Curiae for the Supreme Court, *United States v Microsoft*, No. 17-2, p.30.

at all times. This procedure seems essential in the field of criminal law, given the high risk of violations of fundamental rights if a criminal guarantee is breached.

The MLAT system was rejected as a course of action by the US Department of Justice in *Microsoft Ireland* and by the public prosecutor in *Yahoo! Belgium* due to the unnecessary complexities it added. As noted in previous paragraphs, in *Microsoft Ireland,* the personal jurisdiction of the US over Microsoft Corporation was undisputed. Therefore, the Department of Justice disagreed to request Irish assistance through the applicable MLAT,[76] when the storage of data in Ireland "[depended] solely on a provider's business decision, made without a user's knowledge or consent and subject to change at any moment."[77] Moreover, Microsoft's employees could retrieve the data from its storage location in Ireland and restore it again in its US data centers in seconds. The US Government did not believe that Irish assistance through an MLAT was necessary to order disclosure of such data.

The Brief for the US Government, submitted to the US Supreme Court in the vacated appeal of the *Microsoft Ireland* case further noted that relying on the MLAT procedure for similar cases would "hamper domestic law enforcement and counterterrorism efforts."[78] In effect, the MLAT in force between the US and Ireland, mirroring other MLATs, establishes that direct communication shall take place only between the US Attorney General and the Irish Minister for Justice.[79] Consequently, the competent LEA would be required to refer the matter to the Attorney General, who would, in turn, seek assistance of his Irish counterparty, under article 5 of the MLAT. The Irish Minister, after assessing the lawfulness of the request, would instruct the competent Irish prosecutor to seek a valid court order under Irish law. Once the order to seek the data held by Microsoft Ireland Operations Ltd. is enforced, the Irish Government would still have to examine the data to determine whether its transfer for disclosure to the US Government is provided for under Irish and EU law.[80] According to records kept by the US Government, MLAT-based

[76] Treaty between the United States and Ireland, on Mutual Legal Assistance in Criminal Matters, 18 January 2001, No. 13137.
[77] United States, Brief for the Supreme Court, *United States v Microsoft*, No. 17-2, p.42.
[78] *Ibid*., p.41.
[79] Treaty Between the United States and Ireland, *supra* note 76, articles 2(2) and 2(3).
[80] P. SWIRE, J. HEMMINGS, "Stakeholders in Reform of the Global System for Mutual Legal Assistance," (2015) 32 *Scheller College of Business Working Paper Series*, p.2.

requests are typically responded after an average delay of 10 months.[81] Conversely, as discussed in Chapter IV below, the Commission's e-Evidence Proposal requires CSPs to respond to LEA orders in 10 days, which can be reduced to 6 hours in urgent cases.[82]

Researchers at CEPS have criticized the US Government's attitude towards the MLAT system. In their view, "there is no evidence substantiating the argument that the EU-US MLAT is ineffective, which would properly justify bypassing its application."[83] Their research points out that some of the causes which lengthens the MLAT procedure in the US are not structural and, thus, may be corrected. In their view, the US has established "informal grounds of review" to reject MLAT requests in which the financial interest is low.[84] Furthermore, US authorities require their foreign counterparties to justify that the requests meet the Fourth Amendment "probable cause" standard, even when this concept is foreign to most practitioners outside the US.[85]

In this regard, the research concludes that there are ways in which the process may be streamlined. In particular, it is claimed that the offices which review the applications sent from other states lack "adequate staffing and financial resources."[86] In addition, MLAT rules could be amended by including priority procedures where assistance is needed for urgent cases such as those related to the freezing of a bank account.[87] EU and US officials could be served with a "Guide for Practitioners" to facilitate understanding of the EU-US MLAT, given the high volume of data flows existing between the two sides of the Atlantic.[88]

These proposals would indeed contribute to reduce the time frames in which MLAT procedures take place. However, it seems far-fetched to argue that the only problem is the "lack of willingness of the relevant authorities" to "make proper and effective use of the

[81] Recommendations of the President's Review Group on Intelligence and Communications Technologies, as quoted in SWIRE and HEMMINGS, *supra* note 80, p.2.
[82] e-Evidence Regulation, *supra* note 13, articles 9(1) and 9(2).
[83] CEPS, *supra* note 43, p.69.
[84] *Ibid*., p.67.
[85] *Ibid*., p.68.
[86] *Ibid.*, p.71.
[87] *Ibid.*, p.68.
[88] As an example, in 2014 alone the British Government sought "consumer data for at least 53,947 separate user accounts controlled by American technology companies." *See* WOODS 2016, *supra* note 3, p.743.

existing criminal justice cooperation tools."[89] In effect, the time needed to receive authorization from all the actors involved (i.e. prosecutors, judges and Ministers from two states) will not likely be as swift as court orders served directly to the CSP. Furthermore, the fact that one central office must receive and process all MLAT requests is likely to result in workload-management policies such as the "informal grounds of review" reported by CEPS.

It is important to note that the rise to the cloud[90] is not yet complete. If users increasingly rely on CSPs to store data, then the required data for law enforcement purposes will increasingly be stored in foreign databases. Hence, the number of MLAT procedures will escalate exponentially. Maintaining a central office capable of diligently processing MLAT requests does not indeed constitute the most affordable option in the hands of governments.

Furthermore, and most importantly, some CSPs are adopting storage models which challenge the most fundamental principle which underlies MLATs: that the evidence sought, e.g. a database or a collection of documents, is located only in one country at a given time. As the US Government argued in *Microsoft Ireland*, companies such as Google "move data all over the world, sometimes breaking it into 'shards' so that different portions of a single email account may be stored in multiple countries at any one moment."[91] In the US Government's view, MLATs were not only a burdensome procedure, but also a completely ineffective tool whenever companies adopt a "Data Shard" storage model. This argument was one of the deciding factors to not extend the Court of Appeal's ruling in *Microsoft Ireland* to subsequent cases involving data held by Google[92]. Indeed, following the MLAT procedure to seek data stored by Google would lead to a "global game of whack-a-mole" insofar as "the only [Google] personnel with the authority to access user communications are located in the United States."[93]

---

[89] *Ibid*., p.70-71.
[90] ANDREWS and NEWMAN, *supra* note 2, p.323.
[91] United States, Brief for the Supreme Court, *supra* note 77, p.15.
[92] A. KIRSCHENBAUM, "Beyond Microsoft: A Legislative Solution to the SCA's Extraterritoriality Problem", (2018) 86 *Fordham Law Review* p.1947.
[93] *Ibid*., p.1947.

MLAT procedures prevent the existence of conflicts of laws insofar the procedure ensures that court orders issued under the laws of the issuing state are compatible with the laws of the receiving state, through the intervention of a judge in this last state. However, in light of the previous considerations, new legal instruments must be used in order to ensure effectiveness of legitimate LEA requests while solving existing conflicts of laws.

3.2. The Unmediated Model (I): International Comity Principles

International comity rules are general principles of law which establish the framework to analyze whether the enforcement of one state's laws should be prevented on grounds that it would breach the laws of a foreign state. Professor Woods has strongly advocated for reliance upon international comity rules in order to solve the conflicts of law which arise when states assert jurisdiction over data. However, it must also be noted that international comity rules lead to unfair outcomes when courts are faced with cases which involve fundamental rights.

Professor Woods' arguments target scholars who believe that clouds should not be subject to territory-based jurisdictions, but only to specialist jurisdictions with exclusive competence over cloud disputes.[94] Woods' research contains a broad list of examples in which US courts have successfully been confronted with conflicts of laws. In these cases, rather than selecting one pre-defined criterion to determine which rules –domestic or foreign– should be applied, courts balance the competing state interests to select the prevalent one in each case.[95] The balancing exercise will sometimes prevent enforcement of US jurisdiction in favor of the prevalent foreign interest and, in other cases, the resulting balance will disregard foreign laws. In Woods' view, it is not necessary to establish a privileged criterion to determine when a state should enforce disclosure orders even if the CSP may be penalized by a foreign state.[96] Courts should have the interpretative margin to balance all the competing interests, in order to determine the situations in which the domestic interests in accessing data should prevail over the interests protected by foreign statutes preventing disclosure.

---

[94] ANDREWS and NEWMAN, *supra* note 2, p.364.
[95] WOODS 2016, *supra* note 3, p.776.
[96] *Ibid.*

An often-cited precedent in support of international comity rules is found in the 1984 case *US v Bank of Nova Scotia*. This case concerns a Canadian bank, which received an order issued by a US court, served to the office in Miami, requesting disclosure of documents which were kept in the bank's offices in the Bahamas and the Cayman Islands. The order breached bank secrecy law in the latter state.[97] In the judgment, the Court of Appeals carried out a balancing exercise by noting that "the interest of American citizens in the privacy of their bank records [under Cayman Islands law] is substantially reduced when balanced against the interests of their own government engaged in a criminal investigation, since they are required to report those transactions to the United States [under US law]."[98] Therefore, the Court ruled that the interest of the US Government was prevalent over Cayman Islands law. Similarly, in *US v Vetco* the Court of Appeals enforced a subpoena which allegedly breached Swiss bank secrecy law.[99] The Court noted that "no case has been cited in which a person has been prosecuted for complying with a [US] court order enforcing [a US tax authority] summons."[100]

Competition law in the EU provides examples of international comity balancing exercises carried out by the EU Court of Justice. In *Geigy v Commission*, a Swiss undertaking claimed that a notification issued by the Commission was void insofar as it breached Swiss law. The Court, first noted that the matter had to be solved "with mutual regard to the spheres of jurisdiction both of the Community and [Switzerland]."[101] However, it concluded that the interest of the EU prevailed insofar as there was no agreement with Switzerland through which to channel the notification.[102] Following Woods' reasoning, there should be no difference whether the evidence sought by the US Government or the European Commission was a physical document or cloud data.[103] Rules on prescriptive jurisdiction and international comity principles suffice to establish limits to the extraterritorial authority of one state.

---

[97] Court of Appeals, Judgment of 14 August 1984, *United States v Nova Scotia*, 11th Circuit, 740 F.2d 817, p.2.
[98] *Ibid*., p.13.
[99] Court of Appeals, Judgment of 11 May 1981, *United States v Vetco*, 9th Circuit, 691 F.2d 1281, p.7.
[100] *Ibid*., p.8.
[101] Judgment of 14 July 1972, *Geigy AG v Commission of the European Communities*, 52/69, EU:C:1972:73, p.11.
[102] *Ibid*., p.11.
[103] WOODS 2016, *supra* note 3, p.776.

These examples show that domestic courts have not hesitated to balance domestic and foreign state interests in order to adjudicate disputes involving conflicts of laws. However, the results achieved by the courts are often far from satisfactory. In the *US v Nova Scotia* case, the Court interpreted the scope of application of Cayman Islands law on the basis that the company concerned was widely present in the US. While arguably the Court could have reached the same conclusion relying upon international principles such as the fight against tax evasion, it did not do so. In cases involving cloud data, the principles concerned will likely involve fundamental rights of privacy. Applying principles of international comity to cloud data would essentially leave the courts of one state to balance the fundamental rights of a foreign state and its own national interest. A critique to this outcome appears when taking into account that "[passing] upon the provisions for the public order of another state is, or at any rate should be, beyond the powers of a court; it involves the relations between the states themselves, with which courts are incompetent to deal."[104] Consequently, principles of international comity must be codified in instruments of international law to prevent courts from interpreting or balancing foreign law when it affects fundamental rights guaranteed in a foreign constitution.

3.3. The Unmediated Model (II): The Budapest Convention

Whenever the enforcement of one state's jurisdiction breaches the laws of another state, courts typically rely on international comity rules to determine the prevalent interest through a balancing exercise. While this mechanism prevents deadlocks whenever a case presents an international element, it grants judges an important margin of discretion. One way to solve these conflicts of laws which is not subject to the court's margin of appreciation involves international agreements. Through bilateral or multilateral negotiations, states can draw the boundaries between the jurisdiction of each state.

Within the existing international instruments, the Council of Europe Convention on Cybercrime,[105] signed in Budapest in 2001 (hereinafter, the "Budapest Convention"), stands as one of the most relevant. The high number of signatories, 47 states, including

[104] Court of Appeals, Judgment 4 February 1929, Moore v Mitchell, 2nd Circuit, 30 F.2d 600, concurring opinion of L. HAND, p.603.
[105] Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001, [2001] No. 185. Hereinafter, "Budapest Convention."

non-members of the Council of Europe, such as the United States or Japan,[106] explains the central role played by the Convention in academic debate. The Convention determines specific cases in which, due to the existence of a reasonable degree of connection between the LEA and a CSP, the applicable domestic law should provide for the disclosure of data. In addition, it also includes provisions which govern the cooperation between LEAs of different states parties. With regards to the first group of rules, two articles will be examined: article 18(1)(a), as the general rule and article 18(1)(b) as a special rule for subscriber data.

The general rule contained in article 18(1)(a) of the Convention regulates production orders issued against CSPs established domestically, regardless of where the data is located. This provision covers all types of computer data (i.e. traffic data, subscriber information or even content data) in the CSP's "possession or control." This article indeed seems to capture a factual situation similar to that in the *Microsoft Ireland* case, where the US Government sought data stored by a US-based undertaking, such as Microsoft Corporation. However, it is unclear whether the notion of "control" would encompass the type of ownership exercised by Microsoft over the data stored in a data center operated by its Irish subsidiary. In effect, under the Convention, it is not sufficient for a CSP to have the technical capacity to access traffic data to conclude that it has "control" over the data. On the contrary, CSPs must be able to control production of data from within the requesting state's territory.[107] Scholars such as Walden have highlighted the possible resemblance between this definition of control and the notion of "controller" under the EU GDPR, insofar as controlling the production of data could be equated as determining the purpose and means of data processing.[108] Following this reasoning, Microsoft Corporation does not seem to "control" production of data by its European customers, who contract cloud space managed by Microsoft Ireland Operations Ltd.[109]

The second rule, namely article 18(1)(b) of the Convention specifically refers to subscriber data. This type of data includes information which concerns the subscriber's identity,

---

[106] Chart of Signatories and Ratifications, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Bxr2Iu09, Accessed 2 May 2018.
[107] Council of Europe, Explanatory Report to the Convention on Cybercrime, adopted in Budapest on 23 November 2001, No. 185, p.173.
[108] I. WALDEN, "Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent", (2011) 74 *Queen Mary School of Law Legal Studies Research Paper*, p.7.
[109] *Ibid*., p.7.

address, payment information or type of service used, as laid out under article 18(3) of the Convention. Subscriber data can be accessed by an LEA even if the CSP is established in a different state, provided that the CSP "[offers] its services in the territory of the Party" and that the data sought relates to such services.

Whenever the sought data does not fall within any of the categories laid down above, states may turn to the clauses governing mutual cooperation under the Convention. These rules contain minimum retention periods[110] and other procedural guarantees intended to preserve the data until international evidence requests are processed (e.g. through MLATs). Within the mutual cooperation clauses, one of the provisions, namely article 32, actually empowers LEAs to seek disclosure of data from a CSP established in a different state party. The conditions, however, include the "voluntary consent" of the "person who has the lawful authority to disclose the data." The impact of the provision is limited insofar as it is unclear whether cloud service providers have the "lawful authority" to disclose data in all cases. Parties, in the Explanatory Report, indicated that this notion would vary "depending on the circumstances, the nature of the person and the applicable law concerned."[111] Its scope of application is, thus, considerably limited.

The previous analysis shows that negotiations at the international level have the capacity to prevent specific conflicts of laws. By establishing common criteria, states may jointly agree to not prevent enforcement of another state's jurisdiction in certain cases. Clauses such as article 18(1)(b) may be construed from this perspective. It can be argued that states agreed to accept jurisdiction of states over subscriber data "possessed or controlled" by foreign service providers which nevertheless offer services in the domestic market. These agreements prevent conflicts of laws insofar as the *locus rei sitae* accepts to not enforce its laws in specific cases and/or when specific guarantees are followed.

The potential benefits of international agreements in order to prevent conflicts of laws have been criticized by scholars precisely taking the example of the Budapest Convention. Critical arguments may be classified into two groups: a) arguments concerning effectiveness of international treaties, and b) arguments concerning the necessity of concluding international agreements.

---

[110] Budapest Convention, *supra* note 105, article 29(7).
[111] Explanatory Report to the Budapest Convention, *supra* note 107, p.294.

The effectiveness of international agreements has been criticized given that agreements tend to establish the "lowest common denominator" to foster international adherence to the text.[112] In the case of the Budapest Convention, parties have not expressly accepted its direct enforceability. Hence, the common rules established by the Convention may be subject to additional requirements, which water down their content. For example, as the Council of Europe has acknowledged, "some Parties may require that [the data] be requested through [MLATs]."[113] In these cases, essentially no procedural advantage for LEAs may be deducted from the Convention.

Furthermore, scholarship has sometimes argued that international agreements are not necessary. According to Professor Woods, these agreements tend to merely codify existing principles of conflicts of laws and rules of international comity, which guide courts in the balancing of the existing interests. While it is likely that the clauses in international agreements stem from principles of common law which have long been applied by local courts, this does not render them inadequate. International agreements harmonize the rules which are used by courts in one state party when facing a conflict of laws with another state party. Given that conflicts of laws are problematic when two applicable laws are contradictory, harmonizing these provisions does not seem at all unnecessary.

In addition, critics indeed highlight severe shortcomings of the Budapest Convention, which has not been able to provide an adequate and workable solution for LEAs in state parties. However, it must be taken into account that the agreement was a very early initiative to tackle cybercrime. As noted in the Explanatory Report, regarding unmediated access to cloud data, parties "ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area."[114] Noting the lack of experience in this field and the difficulty to formulate general rules when the type of cases which will arise is still unclear, parties opted for the minimalistic clauses discussed in the previous paragraphs. However, the negotiations have not yet concluded in this field. In 1 June 2017, the Council of Europe published the draft the Terms of Reference to adopt an

[112] WOODS 2016, *supra* note 3, p.788.
[113] Council of Europe, Production Orders for Subscriber Information, Cybercrime Convention Committee, T-CY(2015)16, 1 March 2017, p.6.
[114] Explanatory report to the Budapest Convention, *supra* note 107, p.293.

Additional Protocol to the Convention which would include more detailed rules on LEA powers over cloud data.[115]

Rules at the multilateral level in principle have the capacity to solve questions of extraterritorial enforcement of jurisdiction, given that they may draw the line between the enforcement jurisdiction of the state conducting the criminal investigation and the jurisdiction of the state in which the CSP and/or the data are located. In addition, whenever two conflicting obligations are imposed, international agreements may include rules to determine which rule shall prevail. Despite the limited scope of the Budapest Convention, the possibility of concluding international agreements should be further explored given that agreements offer reliable solutions for the questions of extraterritoriality, conflicts of laws and protection of user privacy.

[115] Council of Europe, Draft Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, [2017] T-CY (2017)3, version 1 June 2017.

IV. The CLOUD Act and the E-Evidence Proposal

The previous paragraphs offered a comparison between the two logics which guide the disclosure of data in the cloud setting: the mediated model, in which states must seek assistance to obtain access to data stored in a foreign territory; and the unmediated model, in which states may order a domestic establishment of a CSP to disclose the data it controls. Despite negotiations where both the EU and the US discussed reforming the mediated model,[116] the laws recently adopted or proposed in both sides of the Atlantic broadly reflect the principles of the unmediated model.

Following the enactment of the US CLOUD Act, the European Commission decided to release two legislative proposals. Under the e-Evidence Directive, service providers must appoint a representative in the EU to respond to data requests by LEAs. In addition, the proposed Regulation establishes the European Preservation Order and the European Production Order (hereinafter, jointly, "EPO"). EU LEAs will be empowered to rely upon these instruments to request cloud data regardless of the specific location of such data. Starting in Section 4.1. with a brief overview of the recent legislative developments targeting cloud data in the US and the EU, the remaining sections in the chapter analyze some of the key debates concerning these rules. In particular, Section 4.2. assesses whether data protection and privacy rights are appropriately protected in these instruments, Section 4.3. focuses on the codification of principles of international comity and Section 4.4. determines the extent to which the CLOUD Act and the e-Evidence Proposal should be complemented by additional international agreements.

4.1. Overview: A Transatlantic perspective

Both the CLOUD Act and the Commission e-Evidence Proposal roughly follow similar principles in order to ensure timely access to data with criminal relevance. This section will delve into the specificities of each set of rules, starting with the US CLOUD Act and concluding with the European Commission Proposal.

[116] Joint EU-US Statement, following the EU-US Justice and Home Affairs Ministerial meeting of 5 December 2016, 722/16. Accessed on 13 April 2018 on http://www.consilium.europa.eu/es/press/press-releases/2016/12/05/eu-us-ministerial-mtg-on-jha/pdf

The CLOUD Act aims to facilitate US LEA access to data regardless of its location, as well as foreign LEA access to cloud data owned by US service providers. To achieve these objectives, on the one hand, the Act clarifies the powers of US LEAs over data stored in a foreign territory. On the other hand, the Act authorizes the conclusion of executive agreements which allow foreign governments to seek access to data held by US CSPs.[117] In this sense, §103(a) of the CLOUD Act amends the ECPA to indicate that providers of electronic communications services or remote computing services shall comply with production orders regarding data "within such provider's possession, custody, or control, regardless of whether such [data] is located within or outside of the United States."[118] The CLOUD Act does not establish new investigative measures to be used by law enforcement, but rather declares that ECPA instruments (i.e. subpoenas, court orders and court warrants) may target data located in a foreign state.

These provisions only facilitate access to data by US LEAs. Nevertheless, they are coupled with rules which govern the conclusion of executive agreements between the US and foreign nations. Under these international agreements, foreign LEAs are empowered to serve orders directly to a US citizen, a "corporation that is incorporated in the US" or "an unincorporated association a substantial number of members of which are citizens of the US."[119] States with which the US Government has concluded an executive agreement are referred to as "qualifying foreign governments."[120] Qualifying foreign governments must agree to refrain from imposing fines to CSPs who disclose data to the US authorities.[121] In exchange, international comity rules are stricter with regards to these countries, in order to prevent conflicts of laws with America's closest partners.[122]

Shortly after the CLOUD Act was adopted in the US, the European Commission responded by issuing a proposal it had been preparing since 2016.[123] The e-Evidence Regulation establishes two legal instruments –the European Preservation Order and the European Production Order– which empower LEAs to obtain access to data "regardless of

[117] 18 USC §2355(2)(j).
[118] CLOUD Act, *supra* note 9, section 103(a).
[119] 18 USC §2523(a)(2).
[120] 18 USC §2703(h)(1)(A).
[121] 18 USC §2523(b)(4)(I).
[122] 18 USC §2703(h)(2)(ii).
[123] Council Conclusions of 30 May 2016, *supra* note 12, p.3.

[its] location."[124] In addition, the proposed Directive determines that service providers which operate in the Union must appoint a legal representative at least in one of the Member States capable of receiving the EPOs issued by EU LEAs.

Unlike the CLOUD Act, the Commission proposal creates a new legal instrument at the disposal of national LEAs. Consequently, the proposal details the conditions under which the orders may be relied upon by LEAs, including the necessity and proportionality test, the need for prior judicial intervention, enforcement proceedings as well as legal remedies at the disposal of CSPs. The efficiency of the orders is ensured by the quick deadline to which they are subject: CSPs must disclose the required data within 10 days upon the receipt of the EPO or even within 6 hours in some cases.[125] The following sections will address the key issues raised by these rules.

4.2. Privacy Rights and Data Transfers

Legislating in the field of criminal law always involves a careful balance of highly controversial principles. On the one hand, it is important that LEAs have timely access to criminal evidence to prevent and prosecute criminal activity. But, on the other hand, efficiency must not be achieved at the cost of disproportionately limiting fundamental rights. As McNamee indicated, "we cannot keep breaking the law on the basis that we need to uphold the law."[126] To address these questions, this section first lists the obligations imposed by the EU GDPR regarding disclosure of personal data to LEAs. Once the applicability of the GDPR is laid out, the section continues by analyzing the extent to which the CLOUD Act induces US-based CSPs to breach the GDPR. Finally, the analysis turns to the EU e-Evidence Proposal in order to determine whether it solves the risks to privacy posed by the US CLOUD Act.

As noted in Chapter II above, EU law regulates the processing of personal data within the scope of the activities of both entities established in Europe and entities not established in the EU provided, in this last case, that the processing takes place in the context of

[124] e-Evidence Regulation, *supra* note 13, article 1(1).
[125] *Ibid*., articles 9(1)-9(2).
[126] MCNAMEE, *supra* note 15.

commercial or profiling activities.[127] Whenever the processing of personal data is subject to EU law, disclosure of such data to a foreign LEA, even if required by the law of a foreign state, must be subject to the criteria and guarantees laid out under EU law. The Court of Justice, in *Digital Rights Ireland*, noted that the fundamental rights to privacy and data protection were infringed merely "by allowing the competent national authorities to access [the] data."[128]

More specifically, in Opinion 1/15, the Court of Justice indicated that "disclosure" of data to a foreign authority was not the only operation which required compliance with the conditions laid out by EU law. In effect, an analysis under EU law is also needed in two further situations: if the foreign authority would also be given the possibility to "use" the data,[129] and if the disclosure involves a transfer to a third country.[130] Therefore, EU law governs access, transfer and subsequent use of personal data by an LEA. Under EU law, these operations must be completed with due respect to *inter alia* the principles of necessity and proportionality, as interpreted by the EU Court of Justice.[131]

In this context, the GDPR allows CSPs to process personal data following a CLOUD Act order only under one of the six existing legal bases, as laid out in article 6 of the Regulation. The European Commission noted that responses to foreign LEA orders would typically be based on paragraph 'f' of article 6, which protects processing necessary for the "legitimate interests" of the CSP.[132] The Commission considers that the objective of "not being subject to legal action in a non-EU state" constitutes a legitimate interest which allows non-consensual data processing under the GDPR.[133] However, in this case, article 6(f) of the GDPR explicitly refers to the need to ensure proportionality by stating that processing should not be allowed "where such [legitimate] interests are overridden by the interests or fundamental rights and freedoms of the data subject."[134]

---

[127] GDPR, *supra* note 61, article 3.
[128] *Digital Rights Ireland*, *supra* note 66, p.32.
[129] Opinion 1/15 of 26 July 2017, concerning the Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record Data from the European Union to Canada. EU:C:2017:592, p.212.
[130] *Ibid*., p.214.
[131] *Ibid*., p.215.
[132] European Commission, Amicus Curiae, *supra* note 37, p.10.
[133] *Ibid*.
[134] GDPR, *supra* note 61, article 6(f).

The proportionality test has been interpreted strictly in the context of data protection. The Court of Justice has in the past assessed access and use of personal data by weighing up the objectives pursued by the processing of data with factors such as: the delimitation of the categories of data which are processed,[135] the extent to which automated means are involved,[136] the authorities which will be granted access to the data,[137] the retention period,[138] or the disclosure of the data to third parties.[139] Furthermore, when personal data is shared with a foreign public authority, such authority must respect the rights of the data subjects, namely the rights to access and to rectify the data[140] and must ensure that an independent authority oversees the processing activities.[141]

If ever a US court upheld a disclosure order which contained a disproportionately long retention period, in which the receiving authorities were not specifically defined or where the categories of data were overly broad, compliance with the order would induce the CSP to breach EU law. The fact that a US court may review and validate disclosure orders issued in the context of the CLOUD Act does not alter the previous conclusion insofar as article 48 of the GDPR explicitly prohibits data transfers ordered by foreign courts outside the context of an international agreement concluded with the EU (e.g. an MLAT).

Turning now to the EU e-Evidence Proposal, it may be argued that some of the concerns which were highlighted in the previous paragraphs are addressed more successfully. Any act adopted by a Member State in the scope of application of EU law which involves the processing of personal data must be in compliance with EU data protection law and EU fundamental rights. Should an EU LEA enforce an order which breaches EU fundamental rights, the concerned users will be entitled to "effective remedies" under article 17 of the e-Evidence Regulation, without prejudice to the legal remedies established under article 77 and following of the GDPR and article 52 and following of the Police Data Directive,[142] which are not amended by the new rules.

---

[135] Opinion 1/15, *supra* note 129, p.163.
[136] *Ibid*., p.173.
[137] *Ibid*., p.183.
[138] *Ibid*., p.189.
[139] *Ibid*., p.212.
[140] *See Ibid*., pp.218 and following.
[141] *See Ibid*., pp.231 and following.
[142] Directive 2016/680/EU of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation,

The e-Evidence Proposal, however, has been criticized on two grounds. Firstly, it does not aim to protect EU fundamental rights in light of the enactment of the CLOUD Act. Without concluding that the investigative powers of EU LEAs should not be expanded, it must be noted that the e-Evidence Proposal does not include any provision to minimize the risks caused by the adoption of the CLOUD Act in the US. While this is understandable insofar as EU legislative instruments can hardly correct risks caused by foreign statutes, it is important that the Commission complements its Proposal with concrete action to conclude an international agreement with the US.

Secondly, as will be further developed in Section 4.3 below, it must be accepted that under the e-Evidence Proposal it is less likely that an EU CSP will be induced to breach the fundamental rights of a foreign nation, given the inclusion of stronger international comity rules. However, the differences between the EU proposal and the US CLOUD Act do not undermine the existing similarities. Both the EU and the US have broadly relied upon the unmediated model to enable direct access to cloud data. Therefore, adopting the e-Evidence Proposal shortly after President Donald Trump signed the CLOUD Act into law, weakens the value of arguments against the CLOUD Act. It is more difficult for US negotiators to believe that the EU is concerned about the capacity of US courts to uphold LEA orders which breach EU law if the EU has also empowered its own courts to uphold LEA orders which breach the law of other nations. This concern, which Christakis has defined as "dangerous risk of herd behavior,"[143] should be taken into account throughout the legislative procedure to prevent that measures adopted by the EU are seen as identical to the CLOUD Act.

The previous paragraphs show that the proposal adopted by the EU does not infringe upon the fundamental rights of the EU insofar as it does not derogate from the general provisions of data protection law and fundamental rights. Nevertheless, in light of the recent developments in US law, which may pose a threat to EU fundamental rights, the EU

---

detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] O.J. L 119/89.

[143] T. CHRISTAKIS, "Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques," [2017] CEIS & The Chertoff Group White Paper, p.30.

should combine the adoption of the e-Evidence rules with international negotiations to tackle the concerns raised by the CLOUD Act.

4.3. Principles of International Comity

As has been highlighted in the previous section, it is not unlikely that compliance with production orders issued by US LEAs under the CLOUD Act is prohibited under EU data protection law. Should similar situations materialize, both the CLOUD Act and the e-Evidence Regulation contain international comity rules which guide courts in the solution of conflicts of laws. The following paragraphs will analyze the suitability of both sets of rules to successfully solve conflicts of laws, starting with the US CLOUD Act and concluding with the e-Evidence Proposal.

From a preliminary standpoint, the CLOUD Act states that US courts may block enforcement of a US production order if, "based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed."[144] US courts are required to interpret the restrictions imposed by EU law in order to decide upon the validity of a US production order. The interpretation of EU law by a US court must be carried out following the interpretative guides directly laid out in the CLOUD Act. In effect, the Act determines that US courts "shall take into account" *inter alia*: "the interests of the United States, including the investigative interests of the [US Government];" the "interests of the *qualifying* foreign government" (emphasis added); the "likelihood [and] extent of penalties to the provider;" the location and nationality of the subscriber; the nature of the provider's ties to the US, etc.[145] If EU data protection law prohibits the transfer of data to a US LEA, the US court which reviews the LEA production order will be required to balance the "likelihood" and "extent" of "penalties" as a result of breaches of EU data protection law with the "interests" of the US.

The status of fundamental rights in the EU is determined by the EU legal order. Under article 6 of the Treaty on European Union, the CFREU "shall have the same legal value as the Treaties." Hence, fundamental rights must be considered primary law of the Union.

[144] 18 USC §2703(h)(2)(B)(ii).
[145] 18 USC §2703(h)(3).

Article 52 of the CFREU indicates that EU fundamental rights may only be limited if provided for by law, respecting their essence, if the restriction is necessary, proportionate and meets "objectives of general interest recognized by the Union." Given that fundamental rights cannot be interpreted restrictively,[146] the Court of Justice carries out strict interpretations of any provision which constitutes an exception to a fundamental right. In this regard, the proportionality test involves assessing whether a restriction to a fundamental right is strictly necessary to achieve an objective of general interest recognized by the EU. Whenever EU law is applicable, account must not be taken of the fact that the individual may be a citizen of the US to restrict the laws conferred under the Union's legal order. Similarly, the fact that the service provider was first established in America is not relevant for these purposes. Only the interpretative guides laid out under EU law, as stated in the Court's case law, serve to assess whether a fundamental right conferred by the Union's legal order was breached.

The CLOUD Act requires US courts to take into account the penalties which may be imposed on the CSP for breaches of foreign law. If US courts consider that the investigative interest of the US LEA should prevail over possible fines established under the GDPR, CSPs may be forced to choose whether to breach EU or US law. However, EU fundamental rights must not be interpreted in light of the "interests of the United States." Despite that US courts will not likely uphold decisions if they seriously undermine EU fundamental rights, given that both legal systems share a high number of core principles, the CLOUD Act essentially modifies the rules to interpret EU fundamental rights.

Such change may be necessary to articulate a cloud-based market in which jurisdictions are more closely interconnected. It is reasonable that, in certain cases, US production orders are enforced in cases which display close ties to the US and a more tenuous link to the EU. For example, this would happen if all the elements of a criminal case are American, but the data was stored, following a contractual arrangement, in a data center located in the EU. However, the decision to modify the scope and interpretation of EU fundamental rights following the "interest of the United States" must be made by the European legislature. Under article 52 of the CFREU, EU fundamental rights may only be restricted by an EU legislative act.

---

[146] Judgment of 13 May 2014, *Google Spain SL v AEPD*, C-131/12, EU:C:2014:317, p.53.

The Commission e-Evidence Proposal, unlike the CLOUD Act, poses a much more limited threat to other states' fundamental rights. The proposal also follows an unmediated access model, under which it is possible that CSPs are ordered to disclose data to an EU LEA even if such disclosure was prohibited according to the laws of another state. However, the Proposal includes a more comprehensive catalogue of rules on international comity, which provide a more considerate approach to the potential conflicts of laws. Hence, unlike the CLOUD Act, the e-Evidence Regulation does not balance the fundamental rights protected by foreign nations with the interest of the EU LEA. The Regulation makes a distinction between conflicts of laws involving fundamental rights or fundamental interests in the field of national security or defense of another state, and conflicts which involve other provisions.[147]

Under article 15 of the proposed Regulation, if the service provider considers that a production order breaches the fundamental rights of another state, it may object to its enforcement. An objection would trigger a procedure of judicial review in which the local court is requested to determine whether a "relevant conflict" exists. Should that be the case, the judge must inform the central authorities of the state concerned. If the state concerned objects in the deadline of 15 days, the order will be lifted.[148] These rules aim to prevent EPOs from breaching the fundamental rights of another state. However, it is important to note that the review procedure only takes place after the service provider has objected to the EPO. In this context, it has been argued that the likelihood of CSPs objecting is low given the tight deadlines to which they are subject,[149] the existence of "effective, proportionate and dissuasive"[150] fines for non-compliance,[151] and the fact that EPOs are issued in certificates which do not include an adequate statement of reasons to substantiate an objection.[152]

Conversely, under article 16 of the proposed Regulation, more flexible rules govern conflicts of laws which involve other provisions. In these situations, judges are allowed to

---

[147] e-Evidence Regulation, *supra* note 13, articles 15-16.
[148] *Ibid*., article 15(6).
[149] *Ibid*., article 9.
[150] *Ibid*., article 13.
[151] J. JEPPESEN, G. NOJEIM, "Initial Observations on the European Commission's E-Evidence Proposals," 18 April 2018, Center for Democracy and Technology, p.5.
[152] *Ibid*. *See* also e-Evidence Regulation, *supra* note 13, articles 8-10.

balance the concurring interests to select the prevalent one, as is the case under the CLOUD Act. Hence, even if the EU proposal provides for the interpretation of foreign law in light of domestic interests, it precludes such balancing exercise when fundamental rights protected by foreign nations are involved. This approach may indeed still lead to unfair outcomes in which foreign law is disregarded, but it nevertheless includes stronger guarantees.

4.4. International Agreements

The CLOUD Act authorizes the conclusion of executive agreements with foreign states provided that the Attorney General, "with the concurrence of the Secretary of State," certifies that the foreign state complies with the required levels of protection for privacy, civil liberties, etc.[153] These agreements do not have the effect of ensuring cooperation between LEAs, as MLATs do, but rather of establishing that equal treatment is granted between "qualifying foreign governments" and the US. The agreements would prevent the US Government from imposing penalties upon CSPs which comply with production orders issued by foreign LEAs.[154]

These agreements show the willingness of the US to offer a similar treatment to other states. Given that most CSPs are based in the US, foreign governments will be less likely to oppose US LEAs' access to data stored within their borders if the law equally facilitates foreign LEAs' access to data stored in the US. Nevertheless, this section of the CLOUD Act was the target of most critical voices, from the perspective of US constitutional rights. In this sense, the certification made by the Attorney General regarding privacy and civil liberties' protection in the foreign state may not be "subject to judicial or administrative review."[155]

Similarly, civil rights groups have highlighted that the Attorney General would certify the respect of fundamental rights before the executive agreement is concluded, but not on an individual basis for each case. The CLOUD Act indicates that the qualifying foreign

[153] 18 USC §2523(b).
[154] 18 USC §2511(2)(j).
[155] 18 USC §2523(c). *See* N. GIULIANI, "The Cloud Act Is a Sinister Piece of Legislation", ACLU, 13 March 2018. Accessed on 18 April 2018 on https://medium.com/aclu/the-cloud-act-is-a-sinister-piece-of-legislation-816f7e1fdac4

government shall agree to "periodic review" of compliance with the terms of the agreement.[156] Nevertheless, it does not allow individuals to report fundamental rights breaches in specific procedures. Civil rights activists have pointed to the cases of Poland[157] or Hungary[158] to believe that the absence of a case-by-case evaluation mechanism may enable states where compliance with rule of law becomes increasingly questionable to undermine US fundamental rights.

In the explanatory memorandum accompanying the e-Evidence Regulation, the question of international agreements is addressed. The proposal is described as a first step which deepens the reach of EU law enforcement, provided that the laws of other nations are not breached. Nevertheless, in order to further prevent conflicts of laws, "additional agreements with key partners" may be needed.[159] EU officials should commit to this idea and initiate negotiations with their American colleagues with a view to conclude a binding international agreement between both parties. From a preliminary standpoint, it is important to note that international agreements in the field of law enforcement access to data should be concluded by the EU, and not by its Member States. The EU has indeed acquired the exclusive competence to conclude international agreements in this field, insofar as an agreement could "affect [existing internal EU] rules or alter their scope", in the sense of article 3(2) of the TFEU.[160]

Through international negotiations, the EU could request the US to make an explicit commitment to EU fundamental rights. The potential agreement would affirm that US courts will not apply international comity rules when fundamental rights are involved. Provisions could be included to instruct national courts to seek assistance of the counterparty's central authorities or to initiate an MLAT procedure whenever there are signs or indications which show that fundamental rights or certain essential interests of the other party may be compromised. Only unambiguous clauses in an international agreement are likely to build trust in the digital trade between the two Atlantic powers.

---

[156] 18 USC §2523(b)(4)(J).
[157] GIULIANI, *supra* note 155.
[158] MCNAMEE, *supra* note 15.
[159] e-Evidence Regulation, *supra* note 13, explanatory memorandum, p.11.
[160] CEPS, *supra* note 43, p.77.

Furthermore, with a view to reduce potential conflicts of laws, the EU could agree to reduce the scope of its fundamental rights protections. In that case, the EU could accept the privacy protection offered under US law as equivalent to that of the EU whenever the data sought by US authorities concerns US citizens who have strong ties to the US. This limitation of EU jurisdiction would prevent conflicts of laws when users established in the US self-select a different state of residence in their cloud settings and data is migrated accordingly.[161] As noted in previous paragraphs, this restriction of EU jurisdiction would not necessarily be illegitimate, provided that it has been adopted by the Union legislature.

The potential agreement could also include guarantees concerning fundamental rights, such as due process and judicial review to ensure that any cross-border processing of data would not pose a threat to the fundamental interests of any state. Only through negotiations at the international level would the EU achieve an appropriate balance between the two essential interests with underlie these discussions: the effective prosecution of criminal offences and the adequate protection of the rights to privacy and data protection. Relying on international agreements includes the risk, as Woods pointed out, that demands are typically brought down to the minimum common denominator.[162] Similarly, the EU noted that, in this scenario, the outcome of the solutions "would to a large extent depend on third States"[163] Nevertheless, by establishing the Union's unnegotiable priorities, which are linked to its very constitutional foundations, the remaining clauses could be open to a healthy discussion. In a world in which technology provides users with the experience of ubiquity, states must more than ever remain strongly committed to their fundamental values, yet open to global partnerships.

[161] *Microsoft v Ireland*, *supra* note 6, concurring opinion of E. LYNCH, p.15.
[162] WOODS 2016, *supra* note 3, p.788.
[163] e-Evidence Regulation, *supra* note 13, explanatory memorandum, p.8.

V. Conclusion

The widespread use of cloud computing, fueled by the enormous advantages it brings to users, has generated serious difficulties for criminal investigations worldwide. The "internationalization of personal data"[164] leads to permanent cross-border interactions between domestic individuals and often foreign cloud service providers. In the cloud economy, "a person and his data are often separated by great distances and possibly several jurisdictions."[165] This study has delved into the legal intricacies existing in this field to highlight the legal instruments which allow LEAs to seek access to cross-border cloud data for law enforcement purposes.

Starting from recent case law, such as the *Microsoft Ireland* and the *Yahoo! Belgium* cases, it was inferred that states have a legitimate interest to assert jurisdiction both over criminally relevant data located in a different state and over data located within domestic borders. Whilst it must be accepted that data does indeed pose a challenge to the notion of territory-based jurisdiction, it does not completely undermine it.[166] The notion that an Internet-based jurisdiction[167] is necessary insofar as states are unable to control online behavior would lead to legal uncertainty and inequality, especially when noting that the online and the offline sphere increasingly coexist. So long as strong rules governing conflicts of laws exist, nothing should prevent a state from asserting jurisdiction in order to defend the general interests which it represents.

The debate about state jurisdiction is bound to be recurrent. In the wake of the algorithm-driven economy, and the Internet of Things, the role of the state will be increasingly called into question. In this context, the importance of providing states with the adequate legal tools to swiftly solve jurisdictional conflicts with other states transcends the specific issue of criminal investigations. However, asserting jurisdiction in the cloud environment will only contribute to solidify states' legitimacy as representatives of the general interest if their commitment with fundamental rights is unequivocal and explicit.

---

[164] A. WOODS, "Data Beyond Borders: Mutual Legal Assistance in the Internet Era," [2015] Law Faculty Scholarly Articles, University of Kentucky, p.2, quoting an industry analyst.
[165] WOODS 2016, *supra* note 3, p.743.
[166] *Ibid*., p.729.
[167] ANDREWS and NEWMAN, *supra* note 2, p.364.

For this reason, this study has advocated for the conclusion of international agreements as a tool which can successfully conjugate the need for expedited law enforcement with a strong framework for fundamental rights protection. Despite that the MLAT procedure also provided strong guarantees in the field of judicial cooperation, the rise to the cloud is likely to render it obsolete. It is not only that lengthy procedures are unsuited for the cloud economy,[168] but also that new data management policies, such as the "data shard" model, challenge the very notion that relevant content data (i.e. an e-mail account or a set of documents) are stored in the same one location at a given time.[169] Reliance on international comity procedures, although strongly advocated for by some scholars risks reserving judges too wide a margin of discretion. International comity principles should step aside when fundamental rights are being challenged, given that these rights often constitute the very reason of existence of the state.

After having analyzed the rules enacted by the US and proposed by the EU, it was argued that both parties should initiate formal negotiations with a view to conclude an international agreement. Only when the EU and the US regulate the cooperation between law enforcement and cloud service provides through an international binding agreement will these concerns be adequately solved. To facilitate the development of such an agreement, scholarship should take the lead. By clarifying the instances in which existing rules raise serious concerns regarding fundamental rights, research could highlight the key priorities for negotiators. Further academic development in this field would truly contribute to clarify under what conditions it may be possible for technological innovation and fundamental rights to coexist.

[168] Recommendations of the President's Review Group on Intelligence and Communications Technologies, *supra* note 81.
[169] United States, Brief for the Supreme Court, *supra* note 77, p.15.

VI. Bibliography

6.1. Legislation and International Agreements

European Union Law

Charter of Fundamental Rights of the European Union, 12 December 2012, O.J. 364/01.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016, pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-U.S. Privacy Shield, [2016] O.J. L207/1.

Commission Proposal of 17 April 2018, for a Directive laying down rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, [2018] COM(2018)226 final.

Commission Proposal of 17 April 2018, for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters, [2018] COM(2018)225 final.

Directive 2006/24/EC of 15 March 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive), [2006] O.J. L105/54.

Directive 2014/41/EU, of 3 April 2014, regarding the European Investigation Order in criminal matters, [2014] O.J. L130/1.

Directive 2016/680/EU of 27 April 2016, on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, [2016] O.J. L119/89.

Regulation (EU) 2016/679 of 27 April 2016, 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 (GDPR), [2016] O.J. L119/1.

Treaty on European Union

Treaty on the Functioning of the European Union.

US and Belgian Law

Code d'Instruction Criminelle, 17 November 1808, as amended by the Loi modifiant l'article 46bis du Code d'Instruction Criminelle, 23 January 2007.

Consolidated Appropriations Act, 23 March 2018, US Public Law No. 115-141 (2018).

Electronic Communications Privacy Act 1986, Public Law No.99-508, 18 USC §2701–2712.

United States Code, Office of the Law Revision Counsel of the House of Representatives, as amended in 23 March 2018 by the Consolidated Appropriations Act.

International Treaties and Agreements

Agreement between Eurojust and the United States of America, 6 November 2006.

Agreement between the European Police Office and the United States of America, 6 of December 2001

Agreement between the European Union and the United States of America, on Mutual Legal Assistance between the EU and the USA, 19 July 2003, O.J. L 181/34.

Council of Europe Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001, No. 181.

Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001, No. 185.

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, signed in Strasbourg on 28 January 1981, No. 108.

Council of Europe, Explanatory Report to the Convention on Cybercrime, adopted in Budapest on 23 November 2001, No. 185.

Treaty between the United States and Ireland, on Mutual Legal Assistance in Criminal Matters, 18 January 2001, No. 13137.

6.2. Case Law

Case Law of the Court of Justice of the European Union and the General Court

Judgment of 8 April 2014, *Digital Rights Ireland v Minister for Communications*, C- 293/12 and C- 594/12, EU:C:2014:238.

Judgment of 14 July 1972, *Geigy AG v Commission of the European Communities*, 52/69, EU:C:1972:73.

Judgment of 13 May 2014, *Google Spain SL v AEPD*, C-131/12, EU:C:2014:317.

Judgment of 6 October 2015, *Schrems v Data Protection Commissioner*, C- 362/14, EU:C:2015:650.

Judgment of the General Court of 12 June 2014, *Intel Corporation v European Commission*, T- 286/09, EU:T:2014:547.

Opinion 1/15 of 26 July 2017, concerning the Draft Agreement between Canada and the European Union on the Transfer of Passenger Name Record Data from the European Union to Canada. EU:C:2017:592.

Belgian and French Case Law

Cour de Cassation, Judgment of 1 December 2015, *Procureur-Général c Yahoo! Inc.*, P.13.2082.N.

Cour de Cassation, Judgment of 18 January 2011, *Procureur-Général c Yahoo! Inc.*, P.10.1347.N.

Cour de Cassation , Judgment of 4 September 2012, *Procureur-Général c Yahoo! Inc.*, P.11.1906.N.

Tribunal de Grande Instance de Paris, Judgment of 22 May 2000, *UEJF-LICRA v Yahoo!*, 00/05308-00/05309.

US Case Law and Litigation Documents

Bundesverband der Deutschen Industrie, Amicus Curiae for the Supreme Court, *United States v Microsoft*, No. 17-2.

Court of Appeals, Judgment of 14 July 2016, *Microsoft Corporation v United States*, 2nd Circuit, 14-2985.

Court of Appeals, Judgment 4 February 1929, Moore v Mitchell, 2nd Circuit, 30 F.2d 600.

Court of Appeals, Judgment of 13 May 1976, *United States v Field*, 5th Circuit, 532 F.2d 404.

Court of Appeals, Judgment of 14 August 1984, *United States v Nova Scotia*, 11th Circuit, 740 F.2d 817.

Court of Appeals, Judgment of 11 May 1981, *United States v Vetco*, 9th Circuit, 691 F.2d 1281.

European Commission, Amicus Curiae for the Supreme Court, *United States v Microsoft*, No. 17-2.

Ireland, Amicus Curiae for the Supreme Court, *United States v Microsoft*, No. 17-2.

Microsoft Corporation, Brief for the Supreme Court, *United States v Microsoft*, No. 17-2.

Supreme Court, Judgment of 16 May 1827, *The Antelope*, 25 U.S. 546.

Supreme Court, Order of 17 April 2018, *United States v Microsoft*, No. 17-2.

United States, Brief for the Supreme Court, *United States v Microsoft*, No. 17-2.

6.3. Policy Documents and Reports

European Union Institutional Studies and Publications

Article 29 Data Protection Working Party, EU-US Privacy Shield – First annual Joint Review, 28 November 2017, [2017] WP 255.

Article 29 Data Protection Working Party, Opinion 05/2012, 1 July 2012, on Cloud Computing, [2012] WP 196.

Council Conclusions of 9 June 2016, on improving judicial cooperation in cyberspace, [2016] 9579/16.

Council Draft Minutes of 12 July 2016, 3473rd meeting of the Council of the European Union (Justice and Home Affairs), held in Luxembourg on 9 and 10 June 2016, [2016] 10115/16.

Commission Communication of 25 October 2016, Commission Work Programme 2017, [2016] COM(2016) 710 final.

Commission Communication of 20 April 2016, delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union, [2016] COM(2016) 230 final.

Commission Communication of 28 April 2015, The European Agenda on Security, [2015] COM(2015) 185 final.

Commission Inception Impact Assessment, 3 August 2017, Improving cross-border access to electronic evidence in criminal matters, [2017] 3896097.

Commission Non-paper on improving cross-border access to electronic evidence. Accessed on 25 April 2018 on https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

Commission Non-paper of 7 December 2016, Progress Report following the Conclusions of the Council on Improving Criminal Justice in Cyberspace, [2016] 15072/1/16.

Commission Technical Document on Measures to improve cross-border access to electronic evidence for criminal investigations. Accessed on 15 March 2018 on https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf

Joint EU-US Statement of 5 December 2016, following the EU-US Justice and Home Affairs Ministerial meeting, [2016] 722/16. Accessed on 13 April 2018 on http://www.consilium.europa.eu/es/press/press-releases/2016/12/05/eu-us-ministerial-mtg-on-jha/pdf

Council of Europe Papers and Publications

Council of Europe, Criminal Justice Access to Data in the Cloud: Challenges, Cybercrime Convention Committee, Discussion Paper, [2015] T-CY(2015)10.

Council of Europe, Criminal Justice Access to Data in the Cloud: Cooperation with Foreign Service Providers, Cybercrime Convention Committee, Background Paper, [2016] T-CY(2016)2 provisional.

Council of Europe, Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY, Cybercrime Convention Committee, [2016] T-CY(2016)5 provisional.

Council of Europe, Draft Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime, [2017] T-CY (2017)3, version 1 June 2017.

Council of Europe, Production Orders for Subscriber Information, Cybercrime Convention Committee, Guidance Note No. 10, [2017] T-CY(2015)16.

Council of Europe, Rules on Obtaining Subscriber Information, Cybercrime Convention Committee, [2014] T-CY(2014)17.

United States Government Publications

National Institute for Standards and Technology, The NIST Definition of Cloud Computing, US Department of Commerce, [2011] 800-145.

US Department of Justice, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities. Accessed on 26 April 2018 on https://www.justice.gov/archive/olp/rpt_to_congress.htm

Policy Papers and Media

American Civil Liberties Union, Letter Opposing CLOUD Act, 12 March 2018. Accessed on 26 April 2018 on https://www.aclu.org/letter/coalition-letter-cloud-act

S. CARRERA, G. GONZÁLEZ FUSTER, E. GUILD, V. MITSILEGAS, "Access to Electronic Data by Third-Country Law Enforcement Authorities" [2015] *Centre for European Policy Studies*.

N. GIULIANI, "The Cloud Act Is a Sinister Piece of Legislation", 13 March 2018, ACLU. Accessed on 26 April 2018 on https://medium.com/aclu/the-cloud-act-is-a-sinister-piece-of-legislation-816f7e1fdac4

N. GULYAEVA, M. SEDYKH, "Russia Enacts Data Localization Requirement; New Rules Restricting Online Content come Into Effect," 18 July 2014, *Hogan Lovells Chronicle of Data Protection*. Accessed on 21 April 2018 on https://www.hldataprotection.com/2014/07/articles/international-eu-privacy/russia-enacts-new-online-data-laws/

L. HURLEY, "U.S. top court rules that Microsoft email privacy dispute is moot," 17 April 2018, *Reuters*. Accessed on 26 April 2018 on https://www.reuters.com/article/us-

usa-court-microsoft/u-s-top-court-rules-that-microsoft-email-privacy-dispute-is-moot-idUSKBN1HO23S

J. JEPPESEN, G. NOJEIM, "Initial Observations on the European Commission's E-Evidence Proposals," 18 April 2018, Center for Democracy and Technology

O. KERR, "What legal protections apply to e-mail stored outside the US?", 7 July 2014, *The Washington Post*. Accessed on 22 April 2018 on https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/?noredirect=on&utm_term=.fa87a2e88ea6

S. PEIRROU, "Le projet de règlement « E-evidence » (preuves électroniques) présenté par la Commission européenne : un « Cloud Act » européen," 24 April 2018, GDR-ELSJ. Accessed on 25 April 2018 on http://www.gdr-elsj.eu/a-propos-du-gdr/presentation/

Responses to e-Evidence Inception Impact Assessment

ACT The App Association, Comments on the Inception Impact Assessment regarding Obstacles to Accessing Electronic Evidence Across Borders in Criminal Investigations, 20 February 2017. Accessed on 21 March 2018 on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6814_en

BSA The Software Alliance, BSA feedback on European Commission 'inception impact assessment' on 'Improving cross-border access to electronic evidence in criminal matters', 30 August 2017. Accessed on 1 March 2018, on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6804_en

Cloudflare, Response to Inception Impact Assessment, August 2017. Accessed on 16 February 2018 on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6791_en

Georgia Institute of Technology, Submission of the Cross-Border Requests for Data Project of the Georgia Institute of Technology, 31 August 2017. Accessed on 3 March 2018 on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6812_en

Microsoft Corporation, "Impacts of e-Evidence on the Digital Economy", 31 August 2017. Accessed on 26 February 2018 on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6811_en

Syntec Numérique, Feedback on e-Evidence Public Consultation, 31 August 2018. Accessed on 25 February 2018 on https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097/feedback/F6807_en

6.4. Interviews and Conferences

CDPD Conference, "towards a European Production Order?", 31 January 2018. Accessed on 25 April 2018, https://www.youtube.com/watch?v=8z6Cx7qLLHg

6.5. Academic Studies

Law Review Articles

D. ANDREWS, J. NEWMAN, "Personal Jurisdiction and Choice of Law in the Cloud", (2013) 73 *Maryland Law Review*.

P. BELLIA, "Chasing Bits Across Borders", (2001) 454 *Notre Dame Scholarly Works*.

S. CARRERA, G. González FUSTER, E. GUILD, V. MISTILEGAS, Access to Electronic Data by Third-Country Law Enforcement Authorities, [2015] CEPS.

Z. CLOPTON, "Territoriality, Technology, and National Security", (2016) 83 *University of Chicago Law Review*.

T. CHRISTAKIS, "Données, extraterritorialité et solutions internationales aux problèmes transatlantiques d'accès aux preuves numériques," [2017] *CEIS & The Chertoff Group White Paper*.

C. COCQ, "EU Data Protection Rules Applying to Law Enforcement Activities Towards an Harmonised Legal Framework?", (2016) 7 *New Journal of European Criminal Law*.

R. COHEN-ALMAGOR, "Freedom of Expression, Internet Responsibility and Business Ethics: The Yahoo Saga and its Implications", (2012) 106 *Journal of Business Ethics*.

A. COLANGELO, "What is Extraterritorial Jurisdiction", (2014) 99 *Cornell Law Review*.

J. DASKAL, "The Un-Territoriality of Data", (2015) 125 *The Yale Law Journal*.

W. DODGE, “Breaking the Public Law Taboo”, (2002) 43 *Harvard International Law Journal*.

J. GOLDSMITH, “Against Cyberanarchy”, (1999) 40 *Chicago Law School Publications*, Occasional Papers.

P. HERT, M. KOPCHEVA, “International Mutual Legal Assistance in Criminal Law made Redundant: A Comment on the Belgian Yahoo! Case,” (2011) 27 *Computer Law & Security Review*.

W. HON, C. MILLARD, I. WALDEN, “The Problem of 'Personal Data' in Cloud Computing - What Information is Regulated?”, [2011] *Queen Mary University Cloud Legal Research Papers*.

D. JOHNSON, D. POST, “Law and Borders: The Rise of Law in Cyberspace”, (1996) 48 *Stanford Law Review*.

I. KATTAN, “Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud,” (2011) 13 *Vanderbilt Journal of Entertainment & Technology Law,*

O. KERR, “The Fourth Amendment and the Global Internet”, (2015) 67 *Stanford Law Review*.

O. KERR, “The Next Generation Communications Privacy Act”, (2014) 162 *University of Pennsylvania Law Review*.

A. KIRSCHENBAUM, “Beyond Microsoft: A Legislative Solution to the SCA’s Extraterritoriality Problem”, (2018) 86 *Fordham Law Review*.

V. MITSILEGAS, The Constitutional Implications of Mutual Recognition in Criminal Matters in the EU, (2006) 43 *Common Market Law Review*.

V. NARAYANAN, “Harnessing the Cloud: International Law Implications of Cloud-Computing”, (2012) 12 *Chicago Journal of International Law*.

P. SWIRE, J. HEMMINGS, “Stakeholders in Reform of the Global System for Mutual Legal Assistance,” (2015) 32 *Scheller College of Business Working Paper Series*.

P. SWIRE, J. HEMMINGS, “Mutual Legal Assistance in an Era of Globalized Communications: The Analogy of the Visa Waiver Program”, (2017) 71 *New York University Annual Survey of American Law*.

I. WALDEN, “Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent”, (2011) 74 *Queen Mary School of Law Legal Studies Research Papers*.

A. WOODS, “Against Data Exceptionalism”, (2016) 68 *Stanford Law Review*.

A. WOODS, “Data Beyond Borders: Mutual Legal Assistance in the Internet Era”, [2015] *Law Faculty Scholarly Articles*, University of Kentucky.

A. WEBER, “The Council of Europe’s Convention on Cybercrime”, (2003) 18 *Berkeley Technology Law Journal*.

Books

E. DE BUSSER, *Data Protection in EU and US Criminal Cooperation*, Maklu, Antwerpen 2009.

J. COLLIER, *Conflict of Laws*, Cambridge University Press, Cambridge 2004.

J. MARTIN, H. CENDROWSKI, *Cloud Computing and Electronic Discovery*, Wiley, New Jersey 2014.

R. WHISH, D. BAILEY, *Competition Law*, Oxford University Press, Oxford 2015.