Transatlantic challenges in access to electronic evidence: Conflicting obligations under the Stored Communications Act and the General Data Protection Regulation

LL.M. Law and Technology
Tilburg Institute for Law, Technology and Society, Tilburg University
Andreas Gruber
Snr 2030085
June 2019
Supervisor: Prof. Dr. Eleni Kosta
Second Reader: Assoc. Prof. Robin Pierce JD, PhD

Table of contents

Chapter I – Introduction[1]

1.1. Background

Historically, gathering of evidence in criminal investigations has happened primarily inside the territory of one state. This has however been disrupted by the ever-increasing use of webmail services, instant messaging or social media websites. The data which is created using these services increasingly raises in significance for law enforcement agencies ('LEAs') and has generally been summarized under the term 'electronic evidence' (e-evidence). The providers of these services are often not based in the same jurisdiction as the LEA and moreover store user data not necessarily in the user's home state or the provider's location but potentially in any country in the world, usually based on economic or security considerations. LEAs around the globe thus increasingly urge the need to order data from foreign providers as well as to access data which is stored on the territory of another state.[2]

Access to e-evidence is not only essential for the prosecution of cyber-dependent crimes which directly depend on the internet as such, e.g. distributed denial of service attacks (DDoS attacks) or computer hacking, but for the prosecution of all crimes that make use of the internet in their organisation and implementation (cyber-enabled and cyber-assisted offences).[3] Hence, the scope of stakeholders in the related discussion includes not only LEAs, privacy advocates and the providers, but in a broader sense every user of these services.

It is therefore no surprise that a case in front of the US Supreme Court has received worldwide attention, particularly from the EU due to the leading role of Ireland in the proceedings. The case of *United States v. Microsoft Corp.* ('Microsoft Ireland case') has been rendered moot by the US Supreme Court in April 2018, thereby concluding a lawsuit which has been ongoing since 2013.[4] It concerned the validity of a search warrant issued by a US District Court seeking access to E-mail data of a US citizen who was accused of having committed several minor drug offences, whereas the data was stored on one of Microsoft's servers in Ireland, operated by Microsoft's wholly-owned subsidiary Microsoft Ireland Ltd. Microsoft contested that a US search warrant can encompass the disclosure of user data which is not stored on US territory.

The reason behind the Supreme Court's decision to render the case moot was the enactment of the CLOUD Act in March 2018,[5] which clarified that where a provider of a service that falls under the Stored Communications Act (SCA)[6] is required to disclose user data, this refers to all data which is under its 'possession, custody or control',

[1] I would like to express my gratitude to Prof. Dr. Eleni Kosta for her extensive support and valuable recommendations without which this thesis in the present form would not have been possible. Besides I would like to give thanks to Assoc. Prof. Robin Pierce JD, PhD and Dr. Bo Zhao LLM for likewise providing me with further essential feedback during the drafting process.

[2] UNODC, *Comprehensive Study on Cybercrime, Draft – February 2013* (United Nations New York, 2013) 216; European Commission 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Explanatory memorandum' COM (2018) 225 final 1

[3] David Wall, 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing' in Brownsword, Scotford, Yeung (eds), *The Oxford Handbook on the Law and Regulation of Technology* (Oxford University Press 2017) 7

[4] United States v. Microsoft Corp., 584 U.S. ___ (2018)

[5] Clarifying Lawful Overseas Use of Data Act, Pub.L. 115-141, 132 Stat. 348 (23 March 2018)

[6] Stored Communications Act, Pub.L. 99-508, 100 Stat. 1848 (21 October 1986)

including data held by their subsidiaries on foreign territory and regardless of the data's location. Whereas the US argues that this amendment merely translates the already well-established status-quo under US law into statutory law, others have argued that it constitutes a significant turn from traditional proceedings under which data held on foreign territory is requested by using Mutual Legal Assistance Treaties (MLAT).[7]

Concerns regarding the extraterritorial reach of production orders under the SCA have been already expressed in several *amici curiae* during the Microsoft Ireland trial, particularly in relation to the conformity of such measures with international law as well as from a data protection and privacy perspective.[8] US-based providers[9] with subsidiaries in the EU that process personal data whose disclosure has been ordered pursuant to the SCA are now faced with conflicting obligations regarding the disclosure of such data to US LEAs, since these are equally protected under the General Data Protection Regulation (GDPR). Accordingly, transfers of personal data by such a subsidiary to third countries, including the US, are only allowed under specific conditions, which are provided in Chapter V of the GDPR. It is highly doubtful, that transfers of personal data pursuant to a production order by a US LEA meets any of these grounds.[10] Rather, according to Article 48 GDPR, transfers of personal data to a third country, merely based on a judgment by a court or a decision of an administrative body of this country, are only permissible when based on an international agreement such as a MLAT.[11]

Although on first glance the current dilemma seems to exist only for US companies with subsidiaries in the EU, legal conflicts in relation to the transfer of personal data processed by a provider subject to the GDPR to the US, solely based on a production order issued by a US LEA, are also provoked by the extraterritorial scope of the GDPR. For the GDPR to be applicable, the geographical location of the data as well as the headquarter of the company are not decisive.[12] Therefore, under certain conditions, also a provider exclusively based on US territory must comply with the GDPR and its rules on transfer of personal data to third countries, while at the same time it is subject to US jurisdiction and the SCA due to the company's location. These contradicting legal frameworks create conflicting obligations for providers, may undermine the rights granted by the GDPR and furthermore may even affect the cooperation between the EU

[7] United States Department of Justice, 'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (Whitepaper 2019) 7

[8] Brief of Jan Philipp Albrecht, Sophie in 't Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016); Brief of the European Commission on behalf of the European Union as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

[9] For the rest of this thesis, the term 'provider' will be used to refer to companies which are subject to the SCA, therefore providers of 'electronic communication services' and 'remote computing services' as defined under US Law. Further elaboration on this will be given under Section 2.5.

[10] Jan Philipp Albrecht et al. (n 8) 18; Article 29 Data Protection Working Party, 'Comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime' (2013) 3

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) [2016] OJ L 119 Article 48

[12] European Data Protection Board, 'Guidelines on the territorial scope of the GDPR (Article 3) - Version for public consultation' (2018) 3/2018 9

and the US in transnational crime prosecution.[13] It therefore becomes apparent that a solution must be found in which the disclosure obligations under the SCA can be reconciled with the conditions for data transfers to third countries in the GDPR.

A possible way out of this dilemma could be brought upon by a new international agreement in which both the EU and the US take part that regulates cross-border production orders by foreign LEAs and the related data transfers. The GDPR does not exclude this option as the MLAT is only listed exemplarily in Article 48. Potentially, such an agreement could thus establish legal certainty for providers, enhance criminal investigations and safeguard the fundamental right to data protection.[14] Several solutions in this respect have been contemplated. The Council of Europe has concerned itself with cross-border access to data in criminal matters already for several years and is currently drafting an additional protocol to the Council of Europe Convention on Cybercrime,[15] which both the US as well as all EU Member States except Ireland and Sweden have ratified.[16] This protocol shall particularly provide an enhancement of international cooperation in prosecution of cybercrimes and thereby address also cross-border access to personal data.[17]

Furthermore, also the EU has released a proposal for a Regulation that addresses cross-border access to electronic evidence, which serves however only as a solution for data requests by European LEAs and does not include the disclosure of personal data to third country LEAs such as in the US. Nevertheless, in the explanatory memorandum the relationship to the US is mentioned and the need for a solution is underlined.[18] Finally, the US has provided its own solution which is as well part of the CLOUD Act. It allows the US to get into bilateral agreements with foreign governments that fulfil certain criteria. Under such a bilateral agreement, LEAs would be permitted to directly order the disclosure of user data of providers in the respective other jurisdiction.

1.2. Objective and research questions

Transfers of personal data to the US have been of high controversy in the EU over the past years, especially since the Snowden revelations in 2013,[19] which illustrated the nearly unlimited access of US Security Agencies to personal data held by US companies. The question has thus been raised, whether the fundamental rights to data protection and privacy under EU law are sufficiently protected in the context of such transfers. These concerns have been best exemplified by the annulment of the Safe-Harbour Decision[20] by the Court of Justice of the European Union (CJEU) as well as the

[13] Robert Currie, 'Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the «Next Frontier»?' (2017) 54 The Canadian Yearbook of International Law 14
[14] Jennifer Daskal, Peter Swire, 'A possible US-EU Agreement on Law Enforcement Acces to Data?' (*Just Security*, 21 May 2018) <https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data> accessed 20 May 2019
[15] Council of Europe, 'Convention on Cybercrime' (2001) CETS No. 185 ('CCC')
[16] Council of Europe, 'Chart of signatures and ratifications of Treaty 185 Convention on Cybercrime' status as of 20 May 2019
[17] Council of Europe Cybercrime Convention Committee (T-CY) 'Summary report of the 1st Meeting of the T-CY Protocol Drafting Plenary' (2017) T-CY (2017)38 4
[18] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM (2018) 225 final Explanatory memorandum 11
[19] In June 2013, former NSA-employee Edward Snowden has leaked several top-secret documents regarding national and international surveillance activities of the United States.
[20] Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2016] ECLI:EU:C:2015:650

strong criticism concerning its successor, the US-EU Privacy Shield.[21] The objective of this thesis is to analyse in detail the current conflict between the disclosure obligations for providers of services that fall under the SCA and the limitations for data transfers to third countries set out by the GDPR. Besides, the feasible options for legitimising such data transfers will be explored as well as the necessary requirements that would have to be fulfilled therefor.
Hence, the thesis will answer the following **main research question**:

> *How can the obligation to disclose user data under the Stored Communications Act be reconciled with the conditions for transfer of personal data to third countries in the General Data Protection Regulation?*

In order to answer this question, several **sub-questions** must be dealt with first:

1. *In which way are providers of services that fall under the Stored Communications Act obliged to disclose user data to US law enforcement agencies?*
2. *How are transfers of personal data to third countries based on a production order by a US law enforcement agency limited under the GDPR?*
3. *What are feasible solutions for the conflict discussed under sub-question 2 and what are the requirements in terms of necessary safeguards that must be considered from a data protection perspective?*

1.3. Significance

Since the enactment of the CLOUD Act, US providers with subsidiaries in the EU find themselves between a rock and a hard place. They are confronted with seemingly contradicting legal obligations, without any option for acting in accordance with both US and EU law. Considering further that LEAs on both sides of the Atlantic will continue to strive for data of the users of these providers, the need for an alternative solution to the existing framework seems compelling. However, it is of utmost importance that in such a solution the protection of the fundamental right to data protection under the European legal framework does not get undermined. Hence, this thesis will play a pioneering role in exploring and proposing the necessary safeguards which must be included in such a solution.

1.4. Preliminary remarks and limitations

The scope of this thesis focuses on the disclosure obligations of providers under the SCA that encompass personal data protected under the GDPR. The converse way of European LEAs requesting data from US-based providers will not be analysed in detail. Moreover, this thesis addresses the issue mainly from a data protection perspective. Hence, legal questions regarding the execution of extraterritorial criminal investigation powers will only be touched upon to the extent necessary in terms of answering the research questions.

[21] Case T-670/16 *Digital Rights Ireland v Privacy Shield* [2017] ECLI:EU:T:2017:838

1.5. Methodology

This thesis is primarily based on doctrinal legal research on statutory legislation, case law and academic literature on data protection law in the EU as well as criminal and privacy law in the US with a focus on transfer of personal data to third countries. An in-depth legal analysis of the relevant provisions of the SCA after its amendment by the CLOUD Act will be conducted and it will be examined whether the conditions set up therein can be reconciled with the GDPR. Moreover, the existing legal framework for transferring personal data to US law enforcement agencies under the Mutual Legal Assistance Treaty procedure as well as the relevant provisions of the Council of Europe Convention on Cybercrime will be explored and critically evaluated.

When elaborating an alternative solution, recent legal initiatives both under the UN and the Council of Europe framework will be assessed. The primary focus will be directed however towards evaluating the conditions provided by the CLOUD Act under which the US would enter into a bilateral agreement that establishes reciprocal production orders. When compiling the necessary safeguards that such an agreement must include, the conditions for data processing in the context of law enforcement under EU law, stipulated in particular in the Law Enforcement Directive[22] and the Commission's proposal for a Regulation on a European Production Order[23] and the relevant jurisprudence of the European Court of Justice and the European Court of Human Rights (ECtHR) will be taken into account as well as existing legal frameworks for data transfers between the US and the EU in the law enforcement context such as in particular the EU-US Data Protection Umbrella Agreement.[24]

1.6. Chapter overview

This thesis will be structured in the following way: After the Introduction (1) the current legal framework for disclosure of personal data under the Stored Communications Act as amended by the CLOUD Act will be explored and the related international legal framework on cross-border access to personal data will be evaluated (2). Afterwards the limitations on data transfers to third countries based on a production order by a foreign LEA under the EU data protection framework will be illustrated and the conflict between the SCA and the GDPR will be explicated (3). The following chapter will turn to an assessment of a possible solution to the established conflict in the scope of an international agreement between the EU and the US and the appropriate safeguards for such an agreement will be compiled (4). Ultimately, based on the result of the previous chapters, the conclusion will recapitulate the legal conflict, explicate to what extent an international agreement can serve as a solution and summarize the necessary safeguards in form of recommendations (5).

[22] Directive (EU) 2016/680 of the European Parliament and of the Council 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] OJ L119/89

[23] Commission (n 18)

[24] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L336/3

Chapter II – Provider obligations to disclose user data to US LEAs

2.1. Introduction

In order to establish the legal conflict which underlies this thesis it is essential to first explore the legal basis under which providers of services that fall under the SCA are required to disclose user data to US LEAs. To this end, this chapter will explore the scope of the relevant legal provisions in the SCA with an emphasis on the amendments brought upon by the CLOUD Act as well as recent US case-law. Afterwards this chapter will examine the international legal framework and evaluate whether it supports the approach taken in the CLOUD Act.

2.2. The increasing significance of electronic evidence

Over the past few years, the importance of access to electronic evidence in criminal proceedings has been ranked high in international policy documents. The term 'electronic evidence' however is not used consistently in all the related discussions.[25] One very general definition refers to it as 'evidence in the form of data generated by or stored on a computer system'.[26] A clear definition of the data categories concerned would however be essential in order to address the potential limitations for production orders by LEAs based on other legal frameworks, most particularly data protection rules.[27]

Albeit the rather vague definition, the vast majority of electronic evidence which is relevant for criminal proceedings is communication data, which under EU law again can be subdivided into subscriber information, traffic data and content data and constitutes personal data in the meaning of the GDPR.[28] Subscriber information thereby is the primarily sought after evidence in criminal proceedings as it often is a prerequisite for further investigations.[29] Since the significance of electronic communication in our daily lives is constantly rising and therewith also the number of crimes, in which the perpetrator makes at least in some form use of electronic communication services in the context of committing the crime increases accordingly, today the vast majority of criminal investigations involves such data.[30]

From a European perspective, the relationship with the US is crucial in this context. This is mainly due to the widespread use of messaging, webmail or social media services of US-based providers, in particular the so-called 'big six' which are Google, Facebook, Apple, Twitter, Yahoo and Microsoft.[31] At the same time however, also US

[25] Commission, 'Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace' COM (2017) 9554/17 6
[26] Council of Europe Cybercrime Convention Committee (T-CY) 'Criminal justice access to data in the cloud: challenges' (2015) T-CY (2015)10 4
[27] Article 29 Data Protection Working Party, 'Statement on Data protection and privacy aspects of cross-border access to electronic evidence' (2017) 4
[28] Commission (n 25) 6
[29] Council of Europe Cybercrime Convention Committee (T-CY) 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' Final report of the T-CY Cloud Evidence Group (2016) T-CY (2016)5 13
[30] Paul de Hert, Cihan Parlar, Johannes Thumfart, 'Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders' (2018) 9 New Journal of European Criminal Law 328
[31] Convention Committee (T-CY) (n 29) 24

LEAs seek access to data processed by a provider in Europe, where many US providers have subsidiaries that operate data centres, in which personal data of relevance for US criminal proceedings may be stored.[32]

2.3. Different forms of accessing electronic evidence

There are in general two ways of how LEAs may access electronic evidence in a cross-border context.[33] Either the LEA can request or order the data from the provider, by using the MLAT procedure or by directly approaching the provider, or the LEA may directly access the data from a computer, e.g. the suspect's mobile phone or laptop.[34] For the matter of answering the research question, only the first way of ordering or requesting the provider to disclose the data is of importance, as this requires an action by the provider which may eventually cause a conflict with other legal obligations.

2.4. The 'Microsoft Ireland case'

The controversies regarding US LEA's cross-border access to data has been best exemplified in the case of *United States v Microsoft Corporation* (the 'Microsoft Ireland case'). The case dates back to a decision of a magistrate judge of the District Court for the Southern District of New York in 2013, to issue a warrant that required Microsoft to seize and produce the contents of one of its E-Mail accounts based on 18 U.S.C. § 2703 which lays down the conditions under which a provider must disclose user data to US LEAs. Microsoft refused to hand over part of the communication content which was stored on one of Microsoft's servers in Ireland operated by Microsoft's wholly-owned subsidiary Microsoft Ireland Ltd., arguing that a US warrant could not apply to data stored on another state's territory.[35] The District Court however turned down this objection, declaring that once the warrant is issued, it has to be seen as a subpoena since it requires Microsoft to act and does not permit the government to conduct a search or seizure abroad. Microsoft, over whom the court has *in personam* jurisdiction, is only required to disclose data inside US territory, whereas the initial location of the data is irrelevant and therefore, the court argued, there is no implication of an extraterritorial effect.[36]

The Court of Appeals for the Second Circuit quashed this decision. It concluded, that the SCA's main focus lays on protecting the user's privacy, for the invasion of which a warrant is necessary.[37] According to the court, the invasion of privacy occurs when Microsoft, in execution of the warrant, accesses the user data and thereby acts as an agent for the government.[38] Since the data is stored on servers in Ireland, this conduct would occur on foreign territory, notwithstanding Microsoft's or the user's location.[39] Such execution of a warrant on foreign territory contravenes the presumption against extraterritoriality under US law, under which the SCA must be interpreted as

[32] Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the U.S. Senate (15 July 2016) 2
[33] Commission (n 25) 4
[34] Convention on Cybercrime of the Council of Europe (CETS No.185) Article 19(2)
[35] Microsoft Corp. v. United States, 829 F.3d 197, 202 (2d Cir. 2016)
[36] In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) 12
[37] Microsoft Corp. v. United States (n 35) 37
[38] ibid 39
[39] ibid

only applying within US territory.[40] Moreover, neither the available case law nor the interpretation of the SCA gives any reason as to why the expressive use of the term 'warrant' in the SCA should be interpreted as a subpoena.[41] The court concluded, that a warrant which compels Microsoft to produce the content of an E-Mail account that is stored abroad constitutes an unlawful extraterritorial enforcement measure and can thus not be issued by a magistrate court.[42]

This result is also in conformity with the analysis by international legal scholars in several *amici curiae* that have been contributed during the trial. According to these it must be borne in mind that the concerned data had been physically encoded into the servers in Ireland and thus must be seen as a physical subject-matter outside US territory that cannot be addressed by a US warrant.[43] Moreover, it has been agreed that executing such a warrant on foreign territory without that state's consent constitutes an extraterritorial enforcement measure which is incompatible with international law.[44] Nevertheless, the decision has also been criticised by US scholars due to its data location driven approach which is considered not suitable anymore in the internet era.[45] The US government contested the decision and referred the case to the US Supreme Court, which however as a result of the enactment of the CLOUD Act, declared the case moot.[46]

It is noteworthy that in another case running parallel to the Microsoft Ireland case the District Court for the Eastern District of Pennsylvania has obliged Google Inc. to hand over communication content relating to a Gmail account, thereby deviating from the judgement discussed above. The main difference of Google's way to store E-Mails compared to Microsoft is that the E-Mails are split into several parts that are stored on different servers around the world. Where the E-Mails are stored is decided by an algorithm, that should ensure the fastest possible provision of the service. According to the District Court, in order to determine where the invasion of the user's privacy took place for which the warrant is necessary, not the location of accessing the data is relevant, but rather the location of the provider and the LEA.[47] A 'search' as mentioned in the Fourth Amendment to the US Constitution, which provides protection from unreasonable search and seizures by the government, only occurs when Google discloses the data and the LEA reviews it.[48] Consequently, the warrant only referred to a permissible domestic action and does not have any extraterritorial effect. The retrieval of the data by Google from one of their servers abroad on the other hand is only viewed by the court to have the *potential* for an invasion of privacy for which no warrant is necessary.[49]

---

[40] ibid 22
[41] ibid 31
[42] ibid 42
[43] Brief of Amici Curiae Fourth Amendment Scholar, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) 11
[44]Anthony J. Colangelo, Austen L. Parrish, 'International Law and Extraterritoriality: Brief of International and Extraterritorial Law Scholars as Amici Curiae (U.S. v. Microsoft)' (2018) 382 SMU Dedman School of Law Legal Studies Research Paper 7 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105491> accessed 20 May 2019; Currie (n 13) 46
[45] Jennifer Daskal, 'Borders and Bits' 71 Vanderbilt Law Review (2018) 197
[46] United States v. Microsoft Corp (n 4)
[47] In re Search Warrant No. 16-960-M-01 232 to Google, 232 F. Supp. 3d 708 (E.D.Pa. 2017)
[48] ibid 23
[49] ibid

The court furthermore concluded that interpreting the provisions differently in this case would lead to an unreasonable result as the government would be prohibited from accessing the data altogether, since different to the Microsoft Ireland case, based on Google's architecture the company is unable to clearly define the location of the concerned data, which makes the MLAT procedure inapplicable.[50]

2.5. Introduction to the Stored Communications Act

The SCA is part of the Electronic Communications Privacy Act[51] (ECPA) and addresses amongst others the compelled disclosure of user data held by providers of electronic communication services and remote computing services to LEAs. According to 18. U.S.C. § 2510, an electronic communication service is defined as 'any service which provides to users the ability to send or receive wire or electronic communications', which includes not only E-Mail services and Internet access services but also text message services or social media websites.[52] The term 'remote computing services' on the other hand according to § 2711(2) encompasses the 'provision to the public of computer storage or processing services by means of an electronic communications system' and therefore in particular includes cloud service providers. Importantly however, US courts often regard companies as both, providers of electronic communication and remote computing services.[53] For instance, a provider of a webmail service provides an electronic communication service when it allows a user to send and receive E-Mails. However, concerning the further storage of the E-Mails on the webserver of the provider after the user has retrieved them it is regarded as a remote service provider.[54]

As regards the compelled disclosure of user data to US LEAs, the SCA provides different requirements under which US LEAs can issue production orders. The lowest standard thereby applies to subscriber information and session metadata, including IP-addresses.[55] For such information an administrative subpoena by a LEA is sufficient, which does not require an approval by a judge.[56] The standards for the issuance of an administrative subpoena are rather low, requiring merely that the information sought by the LEA is 'relevant' for an investigation that is covered by the LEA's enabling law.[57] For message meta-data, such as the sender and/or recipient of a message or the time and date as well as for content data that has either been stored by the provider for over 180 days or already been received by the user, a court order subject to § 2703(d) (a so-called 'd-order') is required.[58] In order to obtain a d-order the LEA must prove 'reasonable and articulable suspicion', which is a higher standard than mere 'relevancy' but less than

[50] In re Search Warrant Google (n 47) 28
[51] Electronic Communications Privacy Act, Pub.L. 99-508, 100 Stat. 1848 (21 October 1986)
[52] Michael E. Lackey, Oral D. Pottinger, 'Stored Communications Act: Practical Considerations' (*LexisNexis*, 22 June 2018) < https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx> accessed 20 May 2019
[53] Crispin v. Christian Audigier, Inc., 17 F.Supp.2d 965 (C.D. Cal. 2010)
[54] United States v Weaver 636 F.Supp.2d 769 (C.D. Ill. 2009)
[55] 18 U.S.C. § 2703(c)
[56] Orin Kerr, 'A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it' (2004) 72 George Washington Law Review 1208, 1219
[57] Francesca Bignami, 'The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens' (Policy Department C of the Directorate General for Internal Policies-European Parliament, 2015) 16
[58] ibid 18

'probable cause', which is required to obtain a search and seizure warrant under the Fourth Amendment. According to the statutory provisions in the SCA, such a warrant based on probable cause is required, when a LEA orders the disclosure of communication content that is stored for less than 180 days and has not already been received.[59]

Nonetheless in 2010 the US Court of Appeals for the Sixth Circuit decided that *any* access to stored E-Mails by LEAs requires a warrant that is based on probable cause, even if these E-Mails have already been opened and/or downloaded by the recipient, as otherwise a violation of the Fourth Amendment would occur.[60] Although this judgment has not yet been implemented into statutory law in the SCA, in practice, access to communication content is today considered permissible only pursuant to a search warrant based on probable cause.[61] Since the reasoning behind this decision however is built on the Fourth Amendment, which in general is not applicable to non-US citizens outside US territory,[62] it seems that EU citizens, who could be affected by a production order after the amendments under the CLOUD Act, do not enjoy this protection.[63]

2.6. The CLOUD Act

As indicated, the US government decided to solve the legal question that arose in the *Microsoft Ireland* case – at least on a domestic level – by enacting a new law. In March 2018 the US Congress passed an omnibus spending bill which included a section that amended the SCA. In reference to its purpose the Act was titled as Clarifying Lawful Oversea Use of Data Act ('CLOUD Act').[64] By an amendment to 18 U.S.C. § 2713 the CLOUD Act requires providers which are subject to US jurisdiction to disclose all information in their 'possession, custody or control' regardless of whether it is 'located within or outside of the United States.'

Although the SCA does not provide a further definition of 'possession, custody or control' it is apparent from other areas of US law, in particular pre-trial discovery rules on electronically stored information in civil and commercial trials, that it refers both to actual possession and ownership as well as the legal right to obtain the data on demand.[65] This typically includes the right of a parent company to obtain information held by a subsidiary.[66] In the context of the CLOUD Act, the US government has

---

[59] Stephen Mulligan, 'Cross-Border Data Sharing Under the CLOUD Act' Congressional Research Service Report prepared for Members and Committees of US Congress' (2018) 5

[60] United States v. Warshak, 631 F.3d 266, 268 (6th Cir. 2010)

[61] Jennifer Daskal, 'Access to Data Across Borders: The Critical Role for Congress to Play Now' (*American Constitution Society for Law and Policy* 24 October 2017) 4 <https://www.acslaw.org/issue_brief/briefs-landing/access-to-data-across-borders-the-critical-role-for-congress-to-play-now/> accessed 20 May 2019

[62] United States v. Verdugo-Urquidez, 494 U.S. 259, 266; Jennifer Daskal, Stephen Vladeck 'Incidental Foreign Surveillance and the Fourth Amendment' in Gray, Henderson (eds.), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017) 103

[63] Judith Rauhofer, Caspar Bowden, 'Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud' (2013) University of Edinburgh School of Law Research Paper Series No 2013/28 22

[64] Clarifying Lawful Overseas Use of Data Act, Pub.L. 115-141, 132 Stat. 348 (23 March 2018) (hereinafter 'CLOUD Act')

[65] In re Bankers Trust, 61 F.3d 465, 469 (6th Cir. 1995)

[66] Tess Blair, Tara S. Lawler, 'Possession, Custody or Control: A Perennial Question Gets More Complicated' *The Legal Intelligencer* (Philadelphia, 5 February 2018) https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/05/possession-custody-or-control-a-perennial-question-gets-more-complicated/ accessed 20 May 2019

confirmed, that a production order under the SCA may concern also data held by a US company's subsidiary in a third country.[67] Such service providers thus cannot use anymore the arguments brought up by Microsoft to refuse the disclosure of information stored on the territory of a foreign state based on the lack of an extraterritorial effect of the SCA.[68] This confirms in essence the position of the US government in the Microsoft Ireland case.[69]

The CLOUD Act also introduced a new statutory right for the concerned provider to challenge a production order concerning communication content based on a perceived conflict with foreign law which would allow the issuing court to quash the warrant.[70] Besides being limited to content data this right is further curtailed by several aspects. First, a provider may only challenge a warrant if such concerns a person which is neither a citizen nor permanent resident of the US.[71] Secondly, only a conflict with laws of a 'qualifying foreign government' may be considered. A qualifying foreign government is such with whom the US has entered into a bilateral agreement on access to data in criminal proceedings.[72] Finally, even if all requirements are fulfilled, the court may take into account several criteria laid down in the CLOUD Act in order to assess whether to quash the warrant, including the likelihood and extent of penalties the provider might face, the importance of the information for the on-going investigations and the likelihood of timely and effective access to the information by other means.[73]

Interestingly for the matter of this thesis, such conflict of law could particularly be triggered by foreign data protection laws.[74] It is however noteworthy that so far no US provider has challenged a SCA production order based on a comity claim,[75] as even in the Microsoft Ireland case, the applicant did not allege that a legal conflict exists but rather challenged the territorial reach of the warrant.[76] The reason for this strategy however was that with this claim Microsoft could directly challenge the basis in US law rather than relying on the comity analysis by the court with regards to a legal conflict.

2.7. International framework for data requests

In international law, two treaties are of importance as regards cross-border access to information by US LEAs. On the one hand these are MLATs between the US and EU Member States; on the other hand, two provisions of the Council of Europe Convention on Cybercrime, Article 18 on production orders and Article 32 on trans-border access to stored computer data, must be considered.

---

[67] United States Department of Justice, 'Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act' (Whitepaper 2019) 17
[68] Orin Kerr, *Computer Crime Law* (4th edn, American Case Book Series 2018) 34
[69] Jennifer Daskal, 'Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0' (2018) 71 Stanford Law Review 9, 11
[70] 18. U.S.C. § 2703(h)(2)
[71] 18. U.S.C. § 2703(h)(2)(A)(i)
[72] See in detail Chapter IV
[73] 18. U.S.C. § 2703(h)(2)(B)
[74] Jean Galbraith, 'Contemporary practice of the United States relating to international law' (2018) 112 American Journal of International Law 490
[75] Comity is a long-standing common law doctrine, which allows a court in case of conflict of laws to weigh the interests of the United States against those of the foreign government in order to assess a providers obligation to comply.
[76] Daskal (n 69) 12

2.7.1. Mutual legal assistance treaties

Mutual legal assistance in criminal matters essentially refers to a form of state-cooperation in order to collect and exchange information.[77] The concrete form of cooperation is laid down in bilateral treaties, whereas the US currently has such MLATs with 27 EU countries, Croatia being the only one left.[78] Moreover, a framework agreement on mutual legal assistance between the US and the EU has been signed in 2003 and entered into force in 2010.[79] The framework agreement provides minimum requirements which have to be included in each bilateral agreement between a Member State and the US.[80] Most relevant from a data protection perspective, the agreement provides a range of purposes for which the obtained data may be used.[81] For certain cases, a Member State may unilaterally impose additional conditions, however, Member States may not impose any generic restrictions with regards to the legal standards for processing personal data in the requesting state.[82] This essentially means that only in exceptional cases, refusal of assistance based solely on data protection grounds shall be invoked.[83] The first review report by the Commission in 2016 indicated the usefulness and success of the agreement.[84]

Although the concrete MLA procedure between the US and each Member State is complex and diverges in detail from country to country,[85] the general way for requesting information held by a provider is the following: Each state that is part of an MLAT must designate a central authority, which acts as a single point of contact for the other state to handle requests. The LEA in the requesting state thus must first contact its domestic designated authority, which then sends the request to the central authority of the requested state, whereas the concrete MLAT usually sets out the respective formal requirements such a request has to fulfil, for instance, details on the crime for which the evidence is sought and information on the person whose data is concerned.[86] Thereafter the central authority evaluates the request and – in case there is no legitimate ground to deny it – processes it further. In case of a request for disclosure of user data held by a provider, the designated authority either directly orders the provider to disclose the data or forwards the request to the competent domestic authority. After the provider has disclosed the data to the competent authority it is transferred to the requesting state using again the channel between the central authorities. This means, that on a domestic level, the disclosure of data from the provider to the competent authority follows strictly

[77] European Commission, 'Mutual legal assistance and extradition' <https://ec.europa.eu/info/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/mutual-legal-assistance-and-extradition_en> accessed 20 May 2019

[78] United States Department of State 'Foreign Affairs Manual'(FAM) § 962.1 (2018) <https://fam.state.gov/FAM/07FAM/07FAM0960.html> accessed 20 May 2019

[79] Agreement on mutual legal assistance between the European Union and the United States of America [2003] OJ L18/34 (MLA)

[80] Article 3(1) MLA

[81] Article 9(1) MLA

[82] Article 9(2) MLA

[83] Agreement on mutual legal assistance between the European Union and the United States of America [2003] OJ L18/34 Explanatory Note on Article 9

[84] Council of the European Union 'Outcome report, Seminar on the application of the Mutual Legal Assistance and extradition agreements between the European union and the United States of America' (2016) 9519/16 Annex 3

[85] Commission (n 25) 8

[86] AccessNow, 'Mutual Legal Assistance Treaties – Country Profile United States' <https://www.mlat.info/country-profile/united-states> accessed 20 May 2019

the national procedural provisions including all procedural safeguards such as prior review by a court or independent administrative body.

One of the current major disadvantages of this procedure is however that the disclosure of information may take between one and eighteen months.[87] Requests by US LEAs often concern Ireland where many US providers have their European headquarter and data centres. Due to bottlenecks caused by the increasing number of requests which have surpassed the available personnel resources, the time for processing MLAT requests has increased steadily in Ireland over the past years.[88] Another problem is that so far the data location has been considered as the guiding principle to decide which jurisdiction is applicable. Therefore, a LEA may only be able to address the concerned state after it knows on which territory the data is stored. It is thus essential that the concerned service provider first identifies the country where the data is stored and ensures that the data stays in this place and is not moved to another jurisdiction.[89] This may however be difficult in case a provider – for reasons of optimizing the performance of its service – splits the data into several parts which are stored in different data centres in different countries.[90] One example for such method has been already discussed under section 2.4. in relation to Google's webmail service.[91] Such circumstances have been the reason for claims that using the location of the data as the determining factor is obsolete in the internet era and new criteria are necessary.[92]

It follows that sincere improvements of the existing MLAT framework would be required in order to accelerate proceedings. Effectively this could be achieved by a full digitisation of the process and by increasing the personnel and financial resources of the competent authorities.[93] Moreover by issuing guidelines for LEAs, states can contribute to a better education of the competent staff for handling MLAT requests and further speed up proceedings.[94]

2.7.2. The Budapest Convention on Cybercrime

Aside from MLATs, also the Council of Europe Convention on Cybercrime includes two provisions which may allow LEAs to request or order data which is stored in the territory of another party.

---

[87] Council of the European Union, 'Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace' (2016) 15072/1/16 5

[88] Commission (n 25) 9

[89] ibid 8

[90] Cristos Velasco, Julia Hörnle, Anna-Maria Osula, 'Global Views on Internet Jurisdiction and Trans-border Access' in Gutwirth, Leenes, De Hert. (eds) *Data Protection on the Move. Law, Governance and Technology Series, vol 24*, (Springer, Dordrecht 2016) 469

[91] In re Search Warrant Google (n 47) 7

[92] Jennifer Daskal, 'The Un-Territoriality of Data' (2015) 125 Yale Law Journal 326, 397

[93] Council of Bars and Law Societies of Europe (CCBE) 'Position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters' (2018) 2; European Parliament '4th Working paper on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (2018/0108 (COD)) – Relation with third country law' (2019) 5

[94] To this end, the UNODC has published a practical guide for criminal justice officers which explicates the legal procedure in 20 of the most relevant states and provides templates on how to request and produce electronic evidence. See UNODC, 'UNODC and partners release Practical Guide for Requesting Electronic Evidence Across Borders' (1 February 2019) <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html> accessed 20 May 2019

2.7.2.1. Production orders

The Cybercrime Convention provides in Article 18 potentially two legal grounds for LEAs to issue a production order to a provider. Whereas under sub-paragraph (a), a *person* in the ordering party's territory is required to disclose all data in that person's possession or control, sub-paragraph (b) has a narrower scope and requires only *service providers* that offer services in the ordering party's territory to disclose subscriber information in their possession or control. 'Service provider' under the Convention is a broad term, covering all companies that provide communication services by means of a computer system as well as such that store or process data on behalf of its subscribers.[95] It can therefore be concluded that both types of services that fall under the SCA are covered by this term. According to a Guidance Note by the Convention Committee (T-CY) on the disclosure of subscriber information under Article 18, the term 'person' in sub-paragraph (a) includes service providers as well.[96] Considering however that sub-paragraph (b) refers particularly to service providers, it is questionable, whether sub-paragraph (a) was indeed drafted with this intention.[97]

As regards the actual storage location of the subscriber information, the Explanatory Report of the Convention interprets 'possession' of the data as referring to data stored in the ordering party's territory whereas for 'control', the report only requires that the person can produce the data from inside the ordering party's territory, as for instance when using remote data storage facilities.[98] The Guidance Note therefore concludes that the actual storage location of subscriber information is irrelevant as long as the data is in the 'possession or control' of the provider receiving the production order.[99]

Whether this may include information held by a subsidiary on foreign territory is left open. It is however noteworthy that according to the Guidance Note, LEAs may even address production orders under sub-paragraph (b) directly to providers which are 'neither legally nor physically present' in the territory'[100] of the ordering LEA, if they enable individuals in the territory to subscribe to their services and have established a commercial link with the partying state e.g. by providing local advertising of the service. T-CY thus appears to accept that a production order for subscriber information under Article 18 may require a foreign provider to act. This however would be at odds with the requirement in the Explanatory Report that the data must be produced from within the ordering party's territory.[101]

Nevertheless, the Guidance Note appears to partly support the US interpretation of 'possession, custody and control' in § 2713 SCA, at least insofar as subscriber

[95] Paolo Balboni, Enrico Pelino, 'Law Enforcement Agencies' activities in the cloud environment: a European legal perspective' (2013) 22 Information & Communications Technology Law 165, 173
[96] Council of Europe Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note # 10 Production orders for subscriber information (Article 18 Budapest Convention)' (2017) T-CY (2015)16 6
[97] Paul de Hert, Cihan Parlar, Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law' (2018) 34 Computer Law & Security Review 333
[98] Council of Europe, 'Explanatory Report to the Convention on Cybercrime' (2001) CETS No. 185 para 173
[99] Council of Europe Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note # 10 Production orders for subscriber information (Article 18 Budapest Convention)' (2017) T-CY (2015)16 7
[100] Convention Committee (n 96) 6
[101] De Hert (n 97) 333

information is concerned, since both disregard the actual storage location of the data.[102] Yet, it must be kept in mind that a guidance note by the T-CY, although stating that it 'represents the common understanding of the Parties as to the scope and elements of Article 18 Cybercrime Convention',[103] does not constitute a binding international agreement between sovereign states, but is a measure of soft law.[104] Besides, taking into account that the prevailing *opinio iuris* among states seems to remain that unilateral cross-border seizures of data are prohibited under international law, the Convention has to be interpreted against this principle, which can only be overridden by express terms.[105] In this regard, the Guidance Note clearly provides that it does not imply consent by any of the partying states to the enforcement of foreign production orders on their territory.[106] Still, since almost all EU Member States as well as the US have ratified the Convention, the interpretation has considerable significance.

2.7.2.2. Trans-border access to stored computer data with consent

In addition to Article 18, the Convention contains another relevant provision which allows for the voluntary cross-border disclosure of data. Article 32 concerns not just subscriber data but all stored computer data. According to its sub-paragraph (b), a party may without authorisation of the other party,

> (…) access or *receive*, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the *lawful and voluntary consent* of the person who has the *lawful authority to disclose the data* to the Party through that computer system.[107]

Due to its wording 'access or *receive*', the provision includes not only the case of LEAs directly accessing data stored in another jurisdiction, but also receiving this data from a person which has the 'lawful authority' to disclose the data and has 'voluntarily and lawfully consented.' Although in general lawful consent to legitimise the extraterritoriality of such a measure could only be given by a state official of the party where the data is stored, in this context the governments who signed the treaty have provided their prior consent to such measures. The consent of the 'person with the lawful authority' can thus be considered as a trigger that activates this prior consent.[108]

One essential question in this regard is, whether a provider has the lawful authority to disclose data of its users. The Explanatory Report hints in this direction by stating that

> (…) a person's e-mail may be stored in another country by a service provider or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data.[109]

---

[102] Bert-Jaap Koops, Morag Goodwin, 'Cyberspace, the Cloud, and Cross-Border Criminal Investigation the Limits and Possibilities of International Law' (2016) 5 Tilburg Law School Legal Research Papers Series 61

[103] Convention Committee (n 96) 9

[104] De Hert (n 96) 335

[105] United Nations, 'Vienna Convention on the Law of Treaties' United Nations Treaty Series, 1155/331 Article 31(3)(c); Colangelo (n 44) 13

[106] Convention Committee (n 96) 6

[107] Emphasis added

[108] Koops, Goodwin (n 102) 63

[109] Explanatory Report to the Convention on Cybercrime (n 98) para 294

At first this seems to provide a legal basis for disclosing user data that is stored on foreign territory such as under the SCA as amended by the CLOUD Act. However, also the Explanatory Report does not make a final statement on a provider's actual lawful authority to disclose user data stored abroad. The Explanatory Report may be interpreted to consider a provider an authorized person to disclose user data that it stored in a foreign country where this is solely a consequence of its own will.[110] This however precludes cases where the user intentionally stores her data abroad.

In the respective Guidance Note on Article 32, the T-CY further elaborates on this issue and limits this provision significantly by clarifying that a service provider is usually unable to consent validly to the disclosure of their users' data, as they just act as holders of the data for their users and do not control or own the data.[111] Another aspect to consider is that by explicitly referring to the storage of user data in another territory in the Explanatory Report to Article 32, an interpretation of Article 18 that includes data stored abroad as well, such as provided by the Guidance Note, seems to be excessive, as it should not be assumed that the drafters of the Convention wanted to regulated the same issue in two different articles.

Moreover, the Guidance Note states that including a clause in the general terms and conditions of a service provider, by which the user consents that the provider may share the user data with LEAs in case of abuse, does not suffice the requirement for explicit consent which would be necessary in most states.[112] Finally it must be considered, that Article 32 relies on 'voluntary' consent, which precludes the disclosure of data following a production order.[113] Following this reasoning and the Guidance Note, Article 32(b) does not legitimise US LEAs to order a provider to disclose user data stored in the EU, unless the user has provided voluntary and lawful consent herself.

2.8. Conclusion

The amendment to § 2713 SCA in the CLOUD Act stipulates the US doctrine of 'possession, custody and control' of data as the criterion that determines which user data a provider must disclose to US LEAs. A similar approach has been taken in the interpretation of the scope of a production order on subscriber information by the T-CY in its Guidance Note on Article 18 of the Cybercrime Convention. This approach disregards the actual location of the data and has been justified with the 'un-territoriality' of data and the business models of several providers, which store user data scattered over several jurisdictions. Accordingly, such production orders may however include data which is stored outside of US territory and potentially held not by the company receiving the production order but by one of its subsidiaries.

This contravenes the opinion that data must be regarded as a physical subject matter, encoded into a server that is located on the territory of a particular state. Based on the international reactions to the Microsoft Ireland case this still seems to be the predominant legal opinion which is also shared among states.[114] Obliging a provider to disclose data stored in another jurisdiction thus constitutes an extraterritorial

[110] Nicolai Seitz, 'Transborder Search: A new perspective in law enforcement? (2005) 7 Yale Journal of Law and Technology 24, 44
[111] Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note # 3 Transborder access to data (Article 32)' (2014) T-CY (2013)7 7
[112] ibid 6
[113] Koops, Goodwin (n 102) 63
[114] UNODC (n 2) 220

enforcement measure which is not in accordance with international law. As long as no international treaty explicitly overrides this principle, or a shift in international customary law can be established, also the provisions of the Budapest Convention – both Article 18 and 32 – have to be interpreted under this principle and thus do not legitimise the extraterritorial effect of a production order.

In order to avoid such conflicts, cross-border requests for data have hitherto been handled by using the MLAT procedure, which at the same time should safeguard fundamental rights and due process. In this regard, the EU-US MLAT contains restrictions on the use of personal data in order to protect the user's fundamental right to data protection. Considering however the current duration of MLAT requests which make them unattractive for EU and US governments[115] only two options seem to be feasible to avoid further unilateral approaches that endanger fundamental rights: Either the MLAT procedure will be fundamentally improved or a new alternative option which allows for direct cross-border production orders will be found.[116]

[115] Kadzik (n 32) 2

[116] Douwe Korff, 'Key points re the Cybercrime Convention Committee (T-CY) Report: Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group T-CY (2016)5' (16 September 2016) 12 <https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf> accessed 20 May 2019

Chapter III – Limitations on data transfers to third countries pursuant to production orders by foreign LEAs under the GDPR

3.1. Introduction

Despite considerable doubts about its conformity with international law, the CLOUD Act has clarified the extraterritorial effect of the disclosure obligations under the SCA with which providers under US jurisdiction must comply. This chapter will now turn to the question to what extent personal data protected under the GDPR may thereby be affected and address the limitations stipulated by the Regulation. To this end it will be assessed, whether transfers of personal data to the US pursuant to a production order by a US LEA are in accordance with EU data protection law.

3.2. Territorial scope of the GDPR

Before going into detail on the actual requirements for transfer of personal data under the GDPR it is essential to consider that the application of the GDPR is neither triggered by the geographical location of the data nor by the headquarter of the provider.[117] Rather, the territorial scope of the GDPR is defined mainly by two criteria. First, subject to the 'establishment criterion' of Article 3(1) the GDPR applies to processing operations which are carried out in the context of the activities of an establishment of the controller or processor in the Union, regardless of the actual place of the processing operation.[118] An establishment is thereby seen as the effective and real exercise of an activity, even a minimal one, through stable arrangements.[119] Secondly, according to the 'targeting criterion' in Article 3(2) the GDPR also applies in the absence of an establishment in the Union where processing is related to the offer of goods or services to or to the monitoring of data subjects' behaviour in the Union.[120] Due to its extraterritorial scope also the GDPR thus may provoke conflicts with laws of third countries, including the US.[121]

3.3. Requirements for transfer of personal data to third countries

Although initially not much discussed in academic literature,[122] rules on transfer of personal data to third countries have already been included in the 1995 Data Protection Directive (DPD).[123] Alongside the increasing use of foreign services by internet users their relevance has steadily increased in recent years. The spotlight has however only been directed at the respective provisions after the ground-breaking judgement by the CJEU in *Schrems*, in which the Court has not only clarified that transferring personal data to a third country in itself constitutes processing of personal data[124] and

[117] European Data Protection Board (n 12) 9
[118] ibid 4
[119] Case C-230/14, *Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] ECLI:EU:C:2015:639 para 31; Recital 22 GDPR
[120] European Data Protection Board (n 12) 13
[121] Paul de Hert, Johannes Thumfart, 'The Microsoft Ireland case and the cyber- space sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies' (2018) 4 Brussels Privacy Hub Working Paper 5
[122] Dan Jerker B. Svantesson, 'The regculation of cross-border data flows' (2011) 3 International Data Privacy Law 181
[123] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31
[124] *Schrems* (n 20) para 45

accordingly has to comply with the rules on data processing and supervision under the DPD, but furthermore held that it must be ensured that the high level of protection of personal data, which is rooted in Article 8(1) Charter of Fundamental Rights of the European Union (CFR)[125] is also guaranteed when data is transferred to a third country, such as the US.[126] It follows that each transfer of personal data needs to fulfil a two-step test: First, it must be based on one of the legal grounds for data processing and in addition the transfer must comply with the conditions in Chapter V of the GDPR,[127] which aim to ensure that the level of protection ensured in the Regulation does not get undermined when personal data is transferred to third countries.[128]

Considering the importance of setting the conditions for data transfers to third countries in today's interconnected world it is surprising that no unified definition of the term 'data transfer' exists in data protection laws around the world and that no definition of the term is included in Article 4 GDPR.[129] This has also been repeatedly criticized by the European Data Protection Supervisor (EDPS).[130] Due to the technical reality in which processing operations occur on distributed resources worldwide, as the example of Google's webmail service has illustrated, some legal scholars even have argued in favour of abandoning the concept of data transfers entirely and instead establish rules for international data processing.[131]

It is noteworthy that the GDPR does not use the addition 'cross-border' in relation to data transfers to third countries in the sense it is for example used in Article 4(23) when defining 'cross-border processing' which would imply the involvement of more than one sovereign state. Rather the GDPR only refers to the destination of the data, which must be a controller or processor in a third country or an international organisation. The Regulation however does not elaborate on the location of the controller or processor who transfers the data, whether this controller or processor must be located inside the EU or not. Instead it appears that all controllers or processors which are subject to the GDPR must comply with the provisions for data transfers to third countries in Chapter V. This entails that also such controllers, which are subject to the GDPR due to the application of the targeting criterion in Article 3(2) or because they process personal data in the context of the activities of an establishment in the EU, must comply.

On the other hand, considering that the main reason behind including rules on data transfers to third countries in the GDPR is to maintain the high level of protection provided by the Regulation, the destination which triggers the applicability of the conditions in Chapter V can only be a controller or processor in a third country that is *not* subject to the GDPR, since those controllers and processors in third countries that

[125] Charter of Fundamental Rights of the European Union [2012] OJ C326/391
[126] *Schrems* (n 20) para 72
[127] European Data Protection Board, 'Guidelines on derogations of Article 49 under Regulation 2016/679' (2018) 2/2018, 3; Paul Voigt, Axel von dem Bussche *The EU General Data Protection Regulation – A practical guide* (2017) 117
[128] Recital 101 GDPR
[129] Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 International Data Privacy Law 217
[130] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe"' (2012) 17
[131] Paul M. Schwartz, 'Information Privacy in the Cloud' (2013) 161 University of Pennsylvania Law Review 1628, 1629

are already subject to the GDPR must ensure the high level of protection of the Regulation regardless of the conditions in Chapter V.

It follows that personal data which is protected under the GDPR in principle cannot end up at a controller in a third country which is not subject to the GDPR, without having to comply with the conditions in Chapter V.[132] Stating otherwise would deprive this data of its high level of protection which clearly contravenes the general intention behind the rules on data transfers to third countries emphasised in Article 44. Therefore, considering a data transfer to a third country as a transmission of personal data by a controller or processor subject to the GDPR, to a controller or processor in a third country that is not subject to the GDPR – and thus *out of the protection* of the GDPR - appears to be the appropriate interpretation.[133] Moreover, it has been held by the CJEU that making personal data accessible to others on the Internet does not constitute a data transfer.[134] It is however questionable whether this principle also applies to other forms of passive data exchanges. Convincingly the EDPS has held that the fact that personal data is made available with the intention to communicate it to certain recipients in third countries should be considered as a criterion for declaring such processing activities as data transfers.[135]

3.3.1. Two scenarios of data transfers pursuant to disclosure obligations under the SCA

In the context of the disclosure obligations under the SCA, two scenarios can be distinguished in which personal data is transferred by a provider subject to the GDPR to a controller not subject to the GDPR in a third country based on a production order by a US LEA. In the first scenario, the user data of which the disclosure is ordered by the US LEA is processed by a US provider's subsidiary in the EU that is also regarded as the controller under the GDPR, as the entity which defines the means and purposes of the processing operation.[136] If in that case the application of the doctrine of 'possession, custody or control' under US law results in the US provider having the legal right to obtain the sought-after data on demand from its subsidiary, the data transfer occurs between the subsidiary as the controller in the EU and the central office in the US, which subsequently discloses the data to the US LEA. It thereby does not matter whether the data is actively transferred by the subsidiary or directly accessed by the central office, provided that the concerned data is intentionally made available to the central office in the US.

The second scenario concerns the direct disclosure of personal data by a provider subject to the GDPR to a US LEA. Different to its predecessor the DPD, the GDPR does not exclude all processing activities in the course of law enforcement activities, but rather only excludes processing *by* LEAs, for which a separate Directive has been adopted. The disclosure of personal data *to* a LEA is a processing operation undertaken by a controller that falls under the broad definition of 'processing' in Article 4(2)

[132] David Smith, 'ICO Brings Some Welcome Clarification to the GDPR's International Transfer Rules' (*Allen & Overy Digital Hub*, 7 September 2018) <http://aodigitalhub.com/2018/09/07/ico-brings-some-welcome-clarification-to-the-gdprs-international-transfer-rules/> accessed 20 May 2019

[133] For such a definition see e.g. Information Commissioner's Office 'Guide to Data Protection – International transfers' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/> accessed 20 May 2019

[134] Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECR I-12971 para 61

[135] European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the data protection reform package' (2012) 19

[136] Article 4(7) GDPR

GDPR.[137] Such a scenario occurs primarily where the user data sought by the US LEA is processed by a US-based provider that falls under the extraterritorial scope of the GDPR. This can either be the case where although the EU subsidiary is not considered the controller, the personal data is still processed in the context of the activities of this establishment which causes the US-based provider to fall under the scope of the GDPR. The CJEU in *Google Spain* has provided an extensive interpretation of such situations, only requiring that the processing operation is inextricably linked to the activities of the EU establishment.[138] Alternatively, a US-based provider may have to disclose personal data that stems from processing activities which are subject to the GDPR based on the targeting criterion under Article 3(2) that has been described in the previous section. Based on the broad definition of data transfers that has been established, both scenarios should be considered as data transfers to third countries as they constitute the transmission of personal data by a controller subject to the GDPR to a controller which is not covered by the GDPR in a third country.[139]

The cases involving only a US-based provider illustrate that not only the extraterritorial effect of US law creates legal conflicts for providers, but that it needs to be kept in mind, that also the scope of the GDPR, in particular due to the targeting criterion under Article 3(2), may lead to an effect which *Svantesson* has described as 'hyper-regulation', in which the norms of one state order something that the other state forbids, which makes legal compliance impossible.[140] Although the general intension behind the targeting criterion of the GDPR is to ensure a level-playing field for all companies active on the EU market, given its vague formulation and the lack of clear rules in the GDPR on how to resolve such legal conflicts, it amplifies the state of 'hyper-regulation'.[141]

Besides, US courts have in the past established *in personam* jurisdiction over companies established abroad if those have 'sufficient minimum contacts' with the US. Although no case-law on providers of electronic communication or remote computing services appears to exist so far that makes use of this doctrine[142] it is noteworthy that in proceedings regarding websites, US courts have put emphasis on how interactive a website is with users in the US, such as by offering specific promotions for US users.[143] If a European provider fulfils similar criteria it can be expected that a US court would grant the issuance of a direct cross-border production order, which would require a data transfer from the European provider directly to the US LEA. Such a form of data transfer may also be included in a potential EU-US agreement which will be discussed in the next chapter.

---

[137] Article 4(2) GDPR refers to 'disclosure by transmission'

[138] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317 para 56

[139] Liane Colonna, 'Europe Versus Facebook: An Imbroglio of EU Data Protection Issues' in Gutwirth, Leenes, De Hert (eds) *Data Protection on the Move. Law, Governance and Technology Series, vol 24* (Springer, Dordrecht 2015) 44

[140] Dan Jerker B. Svantesson, 'European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments' (2018) 9 Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC) 114

[141] ibid 117

[142] Which is most likely owing to the fact that the overwhelming majority of such providers is established on US territory.

[143] United States DOJ (n 7) 8

3.3.2. Legal grounds for disclosure of personal data

As a preliminary remark it is important to note that the E-Privacy Directive provides special restrictions for processing of communication content and traffic data.[144] However, these rules currently do not apply to personal data processed by OTTs, such as providers of webmail and instant messaging services.[145] Therefor under the current legal regime, only the provisions of the GDPR are applicable for these services. Out of the six legal grounds which are provided for in Article 6(1) GDPR, only three seem to be relevant in relation to the disclosure of personal data based on a production order by a foreign law enforcement authorities:[146] processing due to a legal obligation,[147] in the public interest[148] and in the legitimate interest of the controller or a third party.[149] In exceptional cases, processing with the consent of the data subject could be relevant, e.g. where such data can be used as relieving evidence for the suspect.

3.3.2.1. Processing necessary for compliance with a legal obligation

For a legal obligation to constitute a valid legal basis for the provider, such must be imposed by either Union or Member State law,[150] which generally excludes legal obligations under third country law from the scope. In order for a foreign legal obligation to be a valid legal ground, it needs to be officially recognised by the concerned Member State or by Union law, e.g. by means of an international agreement.[151] This should prevent, that third countries can unilaterally circumvent the EU rules on data protection.[152]

3.3.2.2. Processing necessary for the performance of a task in the public interest

Similarly, processing necessary for the performance of a task in the public interest refers only to interests recognized by Member State or EU law. Tasks carried out in the public interest of a third country in general do not provide a legal basis for data processing.[153] It is however questionable, whether a legal ground would be provided in case a US LEA claims that the public interest concurs the interest of the Member State or the EU, such as in the context of prosecution of international terrorism.[154] Whereas the simple abstract goal of prevention and prosecution of transnational crimes and terrorist offences in each state by itself would not suffice, it may be established on a case-by-case basis that specific and individualized personal data can be disclosed if it is in the shared interest of both states, as long as in full compliance with all other data

[144] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) OJ L201/37
[145] Commission, 'Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC' SWD (2017) 5 final 69
[146] Commission (n 8) 17
[147] Article 6(1)(a) GDPR
[148] Article 6(1)(c) GDPR
[149] Article 6(1)(e) GDPR
[150] Article 6(3) GDPR
[151] Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP 217 19
[152] Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP128 18
[153] Article 29 Data Protection Working Party (n 151) 21
[154] Ian Walden, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Pearson, Yee (eds), *Privacy and Security for Cloud Computing* (Springer, 2012) 307

protection principles, in particular also the rules on data transfer to third countries.[155] Moreover, when interpreting the concept of 'public interest' it is essential to take account of the principles of necessity and proportionality, which require a provider to request a prove of necessity from the LEA that the personal data sought after is in fact necessary for a specific investigation.[156]

3.3.2.3. Processing in the legitimate interest

Lastly, as regards processing in the legitimate interest of the controller or a third party, the service provider has a clear and legitimate interest in complying with its obligations to disclose the data, particularly where it otherwise would fear legal sanctions.[157] Nevertheless, a balance must be struck between this interest and the interests of the data subjects concerned. Although the concrete outcome of this balancing exercise may vary on a case-by-case basis, it can be contemplated that in principle the interests of the data subjects in protection of their data override the interest of the provider not to get fined.[158]

3.3.3. Specific conditions for transfers of personal data to third countries

Chapter V of the GDPR sets out specific conditions under with personal data may be transferred to third countries which aim to ensure that personal data when transferred to third countries is provided with the same level of protection as under the GDPR.[159] First, where the Commission has decided that the third country ensures an adequate level of protection, no further authorisation for a data transfers is required.[160] Currently such an adequacy decision however only exists for data transfers under the EU-US Privacy Shield which concerns data transfers for commercial purposes and not in the law enforcement context.[161]

Alternatively, a controller may also transfer personal data subject to appropriate safeguards, provided that enforceable data subject rights and effective legal remedies are available, such as in particular by means of Standard Contractual Clauses or Binding Corporate Rules.[162] In case of a data transfer between two controllers for the purpose of subsequent disclosure to a US LEA by the recipient, such transfer would however not be subject to none of these safeguards, which furthermore only include transfers for predefined purposes. Finally, the framework seems to lack any clear rules on 'asymmetric' transfers of data, such between a service provider subject to the GDPR and a criminal justice authority in a third country such as the US.[163] It follows, that for

[155] Article 29 Data Protection Working Party (n 151) 16
[156] Article 29 Data Protection Working Party, 'Comments on the issue of direct access by third countries' law enforcement authorities to data stored in another jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime FN 9
[157] Article 29 Data Protection Working Party (n 151) 18
[158] ibid 19
[159] Recital 101 GDPR
[160] Article 45 GDPR
[161] European Union Agency for Fundamental Rights (FRA) *Handbook on European data protection law* (2nd edn Publications Office of the European Union 2018) 257
[162] Article 46 GDPR
[163] Jan Kleijssen, Pierluigi Perri, 'Cybercrime, Evidence and Territoriality: Issues and Options' in Kuijer, Werner (eds), *Netherlands Yearbook of International Law 2016* (Springer 2016) 165; Convention Committee (n 29) 27

the discussed data transfers under Section 3.3.1 the only applicable rules are Article 48 and Article 49.[164]

3.3.3.1. Transfers or disclosures not authorised by Union law

While most of the provisions in Chapter V are based on similar provisions in the former DPD, Article 48 is a new provision that has no counterpart in the former Directive.[165] The article in essence reflects the general position at law hitherto that a controller subject to the GDPR may only transfer personal data to a third country pursuant to a judgment or decision of a judicial or administrative authority of this country where based on an international agreement, such as an MLAT. [166] This preference for transfer of personal data by means of an MLAT had already before been articulated by the Article 29 Data Protection Working Party.[167] Different to the recommendation by the Working Party which demanded an obligatory use of MLATs, the GDPR only lists MLATs as an example for such an international agreement, providing the option that such transfers may be based also on other forms of international agreements.

The article has been drafted in particular to prevent third countries from drafting legislation which aims to 'regulate the processing activities of natural and legal persons under the jurisdiction of the Member States.'[168] Accordingly, Article 48 explicitly only prohibits transfers of personal data by a provider established in one of the Member States based on an order by a US LEA. As regards the transfer of personal data by a provider that is only subject to US jurisdiction, but still falls under the scope of the GDPR, the limitations set out by Article 48 are less clear.

In this context it is useful to further consider the legislative history of the article. Not being part of the initial Commission proposal,[169] a similar article was first introduced by the European Parliament as Article 43a[170] which was a direct reaction to the Snowden Revelations in 2013 and should address the extensive monitoring activities by third countries outside the appropriate channels of international law such as in particular by US intelligence agencies based on the PATRIOT Act and the Foreign Intelligence Surveillance Act (FISA).[171] Whereas the text of its sub-paragraph (1) eventually was roughly adopted as Article 48, one should also take note of Recital 90 of the Parliament's proposal which provided that

[164] Commission (n 8) 12; Brief of EU Data Protection and Privacy Scholars as Amici Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) 9
[165] European Data Protection Board (n 127) 4
[166] Albrecht (n 8) 6
[167] Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' WP 196 23
[168] Recital 115 GDPR
[169] Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final
[170] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)
[171] David Kessler, Jamie Nowak, Sumera Khan, 'The potential Impact of Article 48 of the General Data Protection Regulation on cross border discovery from the US' (2016) 17 Sedona Conference Journal 575, 584

> (…) in cases where controllers or processors are confronted with conflicting compliance requirements between the jurisdiction of the Union on the one hand, and that of a third country on the other, the Commission should ensure that Union law takes precedence at all times.

Although this wording did not find its way to the final text of the Regulation, it may be a hint that initially Article 48 was intended to cover all forms of conflicting obligations for controllers under the GDPR and thus also such where the company is based on US territory.

3.3.3.2. Derogations for specific situations

Despite its general prohibition of data transfers to third countries based on a foreign judicial or administrative order when not based on an international agreement, Article 48 also clarifies that this should be 'without prejudice to other grounds for transfer pursuant to this Chapter.' Thus, also Article 49, which includes derogations for specific situations, might be applicable for such transfers. Under this article, data transfers to a third country can be permissible even if no adequate level of data protection or appropriate safeguards are put in place. Such transfers however shall only be conducted occasionally and not as part of the regular course of actions of the company, since it follows from the very nature of derogations that these are exceptional processing activities.[172] Consequently, particularly large providers that receive a significant amount of data requests on a regular basis cannot rely on this provision as they would not transfer data only occasionally. According to Article 44, the application of all provisions in Chapter V, including Article 49, shall furthermore never lead to a situation where fundamental rights of the data subject might get breached.[173]

Among these derogations, 'transfers necessary for important reasons of public interest' may be applicable for data transfers pursuant to a production order by a US LEA.[174] Similar to what has already been explicated with regards to Article 6(1)(e), it is however not enough that the interest of a third country (e.g. combatting terrorism) also exists in an abstract sense in the Member State.[175] Rather, it must be inferable from EU or Member State law that a data transfer can be made upon this interest.

3.4. Reconciling the provisions

When attempting to reconcile the provisions on compelled disclosure obligations under the SCA with the requirements for data transfers to third countries under the GDPR, it appears that the only form of providing this data which is clearly in line with the European data protection framework are transfers by means of the MLAT procedure, which is even explicitly mentioned in Article 48.[176]

Concerning the transfer of personal data from an EU subsidiary to the US headquarter for the purpose of disclosing the data to a US LEA, neither of the two requirements of the two-step test for the data transfer are fulfilled. On the one hand, the data is transferred based on a legal obligation of a third country, which is not a sufficient legal basis according to Article 6(1)(c) GDPR. Whether it may be permissible due to a legitimate interest of the provider not to get fined in the US has to be evaluated on a case-by-case basis. In addition, on a general basis also no derogation under

[172] European Data Protection Board (n 127) 5
[173] ibid 3
[174] European Commission (n 8) 15
[175] European Data Protection Board (n 127) 10
[176] Albrecht (n 8) 19

Article 49(1)(d) applies where a production order stems from criminal proceedings that only concern US interests such as in the Microsoft Ireland case. Therefore, the transfer also does not fulfil the second criterion.

In relation to the disclosure and transfer of subscriber information, a national provision that implements the Guidance Note on Article 18 CCC and would thus permit such disclosure to foreign LEAs could serve as a legal basis for the provider.[177] As regards the requirements for a data transfer, it is noteworthy that Article 48 GDPR does not refer to MLATs as the only admissible international agreement on which data transfers subject to a foreign judgment or administrative decision can be based. Therefore, also the Cybercrime Convention could be considered as such an international agreement. However, it is still essential that the agreement ensures that the level of protection under the GDPR does not get undermined.

Although the Cybercrime Convention contains a general provision that the application of all powers granted therein are subject to conditions and safeguards that shall provide for the adequate protection of human rights,[178] it must be recalled that according to the CJEU, an agreement which entails the transfer of personal data to a third country must itself provide minimum safeguards that ensure that the requirements stemming from EU data protection law are complied with.[179] Hence, considering that the Cybercrime Convention lacks any such data protection safeguards for data transfers, it cannot be considered to fulfil this criterion and data transfers even when in accordance with the extended scope of Article 18 remain unlawful under the current EU data protection regime.[180]

Finally, direct disclosure of personal data that is protected under the GDPR to a US LEA currently primarily occurs in case a US-based provider is considered the controller of the concerned personal data. For this situation – provided that it is considered a data transfer to a third country, which is not clearly determined under the current legal framework - the GDPR remains unclear on how to proceed. Following a strict interpretation, also in this case, the production order under US law would not be a sufficient legal basis for the data transfer, since it neither constitutes Member State nor EU law as required by Article 6(3) GDPR.

Turning to the conditions in Chapter V, Article 48 does not seem to fit in this situation either, since the data transfer occurs between a provider and a LEA of the same jurisdiction. The ineptness of Article 48 for this situation is further illustrated by the fact that there would be no state which the US could contact by means of an MLAT request in order to receive the data. Considering the purpose of Chapter V, to maintain the high standards of data protection under the GDPR, further guidance on the applicability of the two-step test for data transfers in this context is necessary which would also provide legal certainty for providers. Although this conflict seems to be more of an academic one on first glance, its significance may rise substantially in case the notion of ‘control’ under the CLOUD Act as well as Article 18 CCC will be interpreted as defining either the US-based provider also as the controller in terms of the GDPR in all cases – including where currently the EU subsidiary is considered the controller – or a joint controllership will be established. This would have the effect that the data transfer would in all cases occur between the US-based provider and the US LEA.

[177] Convention Committee (T-CY) (n 26) 33
[178] Cybercrime Convention (n 15) Article 15
[179] CJEU opinion 1/15 [2016] ECLI:EU:C:2017:592 para 141
[180] Walden (n 154) 307

3.5. Conclusion

Aside from the controversy regarding cross-border access to user data from the point of view of state sovereignty, which seems to be the primarily discussed issue in recent literature on this topic, the reconciliation of the contradicting obligations for providers under the SCA and the GDPR in relation to the disclosure of user data is an equally important aspect that has to be addressed. This chapter has shown that out of the existing legal frameworks only the MLAT procedure seems to be in accordance with the GDPR, whereas the remaining legal grounds do not fulfil either one or both necessary criteria of the two-step test. US providers with subsidiaries in the EU thus see themselves between a rock and a hard place. Whereas the central office of these providers is subject to US jurisdiction, and therefor risks a punitive enforcement of a production order in case they do not comply, the European subsidiary falls under the jurisdiction of one of the EU Member States, where the GDPR is directly enforceable. These companies thus risk an administrative fine of up to twenty million euros or 4 % of their total worldwide annual turnover in case they transfer personal data to a third country not in accordance with the conditions in the GDPR.[181]

As regards the direct disclosure of personal data by a US-based provider that is subject to the GDPR, no such catch-22 currently exists in practice because the provider only falls under US jurisdiction and it is questionable to what extent penalties under the GDPR would be enforceable in such a case. Whereas *De Hert* is positive, that enforcement can be guaranteed by using existing instruments of international law[182], others such as *Svantesson* are concerned that the GDPR 'bites off more than it can chew.'[183] If the limitations of the GDPR on such data transfers however cannot be enforced, this could undermine the legitimacy of the Regulation as such, in particular outside of the EU.[184] In this context the effect of Article 27, which requires providers that fall under the GDPR based on Article 3(2) to establish a representative on EU territory, has yet to be seen. In any case, further clarification by the legislator or the EDPB - whose tasks include the provision of guidelines and recommendations to ensure a consistent application of the Regulation[185]- especially on the definition of what constitutes a 'data transfer to a third country' seems necessary in order to provide legal certainty for companies and citizens alike.

[181] Article 83(5) GDPR
[182] Paul de Hert, Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 International Data Privacy Law 242
[183] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 International Data Privacy Law 232
[184] ibid 233
[185] Article 70(e) GDPR

Chapter IV – An international agreement as a possible way forward

4.1. Introduction

Having explicated the conflict between the disclosure obligations under the SCA and the conditions for data transfers to third countries under the GDPR, this chapter will assess the available policy options to address this conflict as well as their feasibility. To this end, recent international developments under the UN framework and the Council of Europe's Cybercrime Convention will be evaluated as well as 18. U.S.C. § 2523 which has been introduced by the CLOUD Act and provides conditions under which the US would get into a bilateral agreement with foreign governments that allows for reciprocal direct production orders to providers in the other jurisdiction. It will be explored to what extent these approaches can resolve the established conflict, and which are the necessary safeguards and limitations that must be considered from a data protection perspective.

4.2. The case for an international agreement

In the light of the conflict being one that involves multiple regulatory aims – primarily criminal prosecution and data protection - an international treaty seems to be the most suitable instrument for a solution, providing the necessary flexibility to address all interests involved.[186] The conditions for data transfers to third countries in the GDPR clearly leave room for such a treaty insofar as sufficient safeguards for the rights of the data subject are included.[187] In addition from a provider's perspective, a solution under an international agreement that has been ratified by the state under whose jurisdiction the provider falls would bring the necessary legal certainty and relieve from impending fines.

4.3. Finding a solution on a UN-level

Given the global availability of electronic communication services and the physical structure of the internet as a worldwide network of cables and servers, finding a solution to access to electronic evidence ideally should involve the whole community of states.[188] On a UN level, a first attempt has been undertaken by the UN-Special Rapporteur on Privacy, who in his Annual Report 2018 presented a 'Draft Legal Instrument on Government-led Surveillance and Privacy' which includes a section on mechanisms for transborder access to personal data.[189]

The draft legal instrument proposes the creation of an International Data Access Warrant (IDAW) that is granted by an International Data Access Authority (IDAA),

---

[186] Erich Schweighofer, 'Principles for US-EU Data Flow Arrangements' in Svantesson, Kloza (eds.) *Trans-atlantic data privacy relations as a challenge for democracy* (Intersentia 2017) 35; Secil Bilgic, 'Something old, something new, and something moot: The Privacy Crisis under the CLOUD ACT' (2018) 32 Harvard Journal of Law & Technology 322, 351

[187] Recital 102 GDPR

[188] Brief of U.N. Special Rapporteur on the Right to Privacy as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) 25; Gail Kent 'Sharing Investigation-Specific Data with Law Enforcement: An International Approach' (2014) Stanford Public Law Working Paper 9 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413> accessed 20 May 2019

[189] United Nations Special Rapporteur on the right to privacy 'Annual Report 2018' A/HRC/37/62 Appendix 7

comprising of judges of separate jurisdictions among which one should be of the jurisdiction from where the request originates, and that is moreover monitored by independent human rights defenders.[190] Such an IDAW may be used by governments in the scope of criminal investigations where several jurisdictional claims over the concerned data are *bona fide* permissible[191] and could also be served directly to a provider in a foreign state who would be assured that disclosing the data is in accordance with domestic as well as international law.[192]

Given the complexity and sensitivity of the topic, agreeing on such a new international agreement in a large forum as the UN will however be a slow and burdensome process.[193] Therefore the most feasible option for an international agreement at the moment would be either an additional protocol to an existing multilateral treaty or a new bilateral agreement between the EU and the US, in which both sides could act as early adopters to find a solution that may serve as a basis for an international approach in the long run.

4.4. An additional protocol to the Cybercrime Convention

Considering that both the US and all EU Member States except for Ireland and Sweden have ratified the Council of Europe Convention on Cybercrime, it stands to reason that a solution could potentially be found therein. The Council of Europe's T-CY Committee has been engaged with finding a solution for cross-border access to electronic evidence since 2011 when it set up an ad-hoc sub-group on jurisdiction and transborder access to data and data flows.[194] Already in 2013 it presented draft elements for an additional protocol to the Cybercrime Convention which should have regulated transborder access to data.[195] The proposed elements however focused mainly on enhancing transborder searches conducted directly by LEAs and did not deal with cross-border requests or orders to providers.[196] Due to a lack of consensus among the parties to the Convention, owing to mistrust among governments after the Snowden revelations as well as in anticipation of the new EU data protection framework which has been proposed by the Commission in 2012,[197] work on an additional protocol was discontinued and further research by a new sub-group called 'Cloud Evidence Group' was proposed instead.[198]

In its final report, the Cloud Evidence Group again suggested an additional protocol to the Convention as a potential solution to resolve the on-going conflict with regards to cross-border access to electronic evidence.[199] This proposal has been taken on in the Terms of Reference of the T-CY for the period September 2017 to December 2019.

---

[190] ibid 32
[191] Brief of U.N. Special Rapporteur on the Right to Privacy as Amicus Curiae (n 189) 26
[192] ibid 35
[193] Koops, Goodwin (n 102) 91
[194] Council of Europe Cybercrime Convention Committee (T-CY) 'Ad-hoc Sub-Group on Transborder Access to Data and Jurisdiction: Terms of Reference (adopted at the 6th Plenary)' (2011) T-CY (2011)05
[195] Council of Europe Cybercrime Convention Committee (T-CY) 'Transborder access and jurisdiction: What are the options? Report of the Transborder Group' (2012) T-CY (2012)3
[196] Council of Europe Cybercrime Convention Committee (T-CY) 'Draft elements of an Additional Protocol to the Budapest Convention' (2013) T-CY (2013)14 5
[197] Council of Europe Cybercrime Convention Committee (T-CY) 'Transborder access to data and jurisdiction: Options for further action by the T-CY Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction' (2014) T-CY (2014)16 13
[198] ibid Appendix 4.2.
[199] Convention Committee (T-CY) (n 26) 40

Consequently, the Committee is currently in the process of preparing the protocol. Given the fact that subscriber information has been identified by the Cloud Evidence Group as the most sought-after information[200] the additional protocol shall primarily focus on enhancing cross-border access to this data category, particularly by simplifying mutual legal assistance requests and allowing for direct cooperation between judicial authorities. In context of the latter, an emergency mutual assistance procedure shall be established, which allows judicial authorities of the partying states to directly cooperate with each other without the involvement of the central authority.[201]

Although the proposal by the Cloud Evidence Group evaluates also the introduction of an international production order based on the principles of the European Investigation Order,[202] the further explanations indicate that such should not be included into the additional protocol but rather be discussed bilaterally among the parties. Besides, since the European Investigation Order is not addressed directly to the provider, but is still an inter-LEA instrument, it would not serve as a solution for data transfers by providers based on foreign production orders.[203] Given furthermore that the additional protocol intends to address only subscriber information, at least at the current stage a solution for the conflict explicated in the first chapters does not seem to be feasible under the Cybercrime Convention framework. Nevertheless, the intended improvements to the MLAT procedure can significantly lower the demand for a system of cross-border production orders. The EU-Commission has already released a recommendation for a negotiating directive which would grant it the permission to negotiate the agreement on behalf of the Union. It should however be underlined that according to the Commission, a potential bilateral agreement between the EU and the US should take precedence over the additional protocol.[204]

4.5. Executive agreements on access to data authorized by the CLOUD ACT

As highlighted above, the CLOUD Act introduced the option for the US government to enter into a bilateral agreement with a 'qualifying' foreign government that should facilitate cross-border data requests.[205] The origins of this provision date back to the results of an ad-hoc Cross-border Data Requests Working Group installed by the US government and in particular a 2015 proposal by *Daskal* and *Woods.*[206] Already before the enactment of the CLOUD Act, in the aftermath of the ruling of the Court of Appeals for the Second Circuit in the *Microsoft Ireland* case, the US government has started negotiations on such a bilateral data-sharing agreement with the

[200] ibid
[201] Council of Europe Cybercrime Convention Committee (T-CY) 'Provisional draft text of provisions: Languages of requests, Emergency MLA, Video conferencing' (2018) T-CY (2018)23 5
[202] Convention Committee (T-CY) (n 26) 41
[203] Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1 Article 7
[204] Commission, 'Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) COM (2019) 71 final 8
[205] Mulligan (n 59) 16
[206] Vivek Krishnamurthy, 'Cloudy with a conflict of laws' (2016) 3 The Berkman Center for Internet & Society at Harvard University Research Publication 10; Jennifer Daskal, Andrew Woods 'Cross-Border Data Requests: A Proposed Framework' (*Lawfare*, 24 February 2015) <https://www.lawfareblog.com/cross-border-data-requests-proposed-framework> accessed 20 May 2019

UK.[207] According to the CLOUD Act, US providers would be permitted to disclose content data directly to foreign governments where a bilateral agreement is in place.[208] This has hitherto been considered to be prohibited under the SCA,[209] although no case-law on the application of the SCA to requests by foreign governments so far exists that would confirm this.[210] The voluntary provision of non-content data from US providers to foreign LEAs has however already been possible under the previous regime.

The CLOUD Act introduces criteria which the legal system of the foreign government must fulfil in order to be certified as 'qualified'. These criteria require that the government provides 'robust substantive and procedural protections for privacy and civil liberties in light of the data collection'.[211] It follows, that the CLOUD Act's primary function is to lay down minimum requirements a foreign government must fulfil in order for the US Congress to endorse the conclusion of a bilateral agreement by the US Attorney General.[212] Such an agreement would regulate cross-border production orders from a LEA in one jurisdiction to a provider based in the other. Conversely, it does not affect in any way the current conditions under which a US LEA can issue a production order under the SCA to a US provider and the respective disclosure obligations that have been explicated in Section 2.5.[213]

4.5.1. The EU as a 'qualifying foreign government'?

In January 2019, the EU Commission has initiated the negotiating process in view of an agreement between the EU and the US on 'cross-border access to electronic evidence for judicial cooperation in criminal matters' by issuing a proposal for a negotiating directive.[214] Since the CLOUD Act itself does not define the term 'foreign government', it is ambiguous whether it includes the EU. Taking into account the ordinary understanding of the term under US law suggests that it refers rather to the government of a particular sovereign state.[215] However, the CLOUD Act only requires that each foreign government with whom the US enters into a bilateral agreement is certified to fulfil the criteria explicated above. This does not prevent the EU to negotiate and conclude the agreement for all Member States including the necessary safeguards.[216] Considering the strong protection of privacy and civil liberties in the ECHR as well as the CFR, in principle all EU Member States should be eligible for

[207] Shelli Gimelstein, 'A location-based test for jurisdiction over data: The Consequences for global online privacy' (2018) 1 University of Illinois Journal of Law, Technology & Policy 22
[208] 18 U.S.C. § 2702(b)(8), 2702(c)(7)
[209] 18 U.S.C. § 2702(a)
[210] Krishnamurthy (n 206) 6
[211] 18 U.S.C. § 2523(b)(1)
[212] Théodore Christakis, 'Lost in the Cloud? Law Enforcement Cross-border Access to Data After the "Clarifying Lawful Overseas Use of Data" (CLOUD) Act and E-Evidence' (*FIC Observatory*, 28 June 2018) <https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/> accessed on 20 May 2019
[213] United States DOJ (n 7) 8; Robert Loeb, 'The CLOUD Act Explained' (*Orrick*, 6 April 2018) <https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained> accessed 20 May 2019
[214] Commission, 'Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters' COM (2019) 70 final
[215] Swire, Daskal (n 13)
[216] ibid

being certified as a 'qualifying foreign government', although the US government has expressed doubts with regards to some Member States.[217]

According to the CJEU, an international agreement that regulates data transfers to third countries must ensure that the provisions guarantee an equal level of data protection as under EU law.[218] A bilateral agreement between the EU and the US may thereby be better suited to preserve the high data protection standards under EU law than several bilateral agreements.[219] This already follows from the stronger negotiating power the EU has compared in particular to smaller Member States. Besides, a multitude of bilateral agreements with different provisions presumably would lead to an unequal level of protection for data subjects throughout the Union.

4.5.2. Lifting legal restrictions on data transfers

One of the prerequisites to get into a bilateral agreement under the CLOUD Act requires a qualifying foreign government to provide 'reciprocal rights of data access'. This entails that the foreign government must remove all legal restrictions that prevent a provider, *including* those subject to US jurisdiction, to respond to valid legal process sought by a US governmental entity under US law.[220] It appears that this would not only include responding to cross-border production orders based on the bilateral agreement, but rather all legal process sought by a US LEA. Agreeing to these terms would thus as well require the removal or amendment of the current restrictions on data transfers to third countries that have been explicated above, which prevent a provider subject to the GDPR from transferring personal data to the US pursuant to a production order by a US LEA.

4.5.3. Exclusion of 'US persons'

Another condition of the CLOUD Act requires that production orders by foreign governments based on the bilateral agreement are limited to non-US citizens and people that do not have permanent residence permission in the US ('non-US persons').[221] For requests that concern US persons, the use of the MLAT procedure shall remain the lawful way of accessing these data.[222] The reason behind the inclusion of this provision was to safeguard the protection of US persons under the Fourth Amendment, which requires a warrant based on probable cause in order to get access to communication content.[223] When interpreting reciprocity of the agreement strictly, this would entail that also US LEAs could not request any content data of citizens or permanent residents of the Member State where the responding provider is situated in and would have to continue to use the MLAT procedure for such requests.[224] The US government has left the door open for such a two-tier system.[225]

---

[217] Christakis (n 212)
[218] Opinion 2015/1 (n 179) para 214
[219] European Data Protection Supervisor, 'Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence' 2/2019 7
[220] 18 U.S.C. § 2523(b)(3)(I) emphasis added
[221] United States DOJ (n 7) 12
[222] ibid
[223] As has been demonstrated in Section 2.5. this refers at least to E-Mail content as well as content data stored for less than 180 days by an electronic communication service provider
[224] Jennifer Daskal, 'Unpacking the CLOUD Act' (2018) 4 eucrim 190, 223
[225] United States DOJ (n 7) 12

This differentiation between citizens and permanent residents on the one side and non-citizens on the other follows from the US approach of considering constitutional rights as 'civil rights'. Accordingly, the purpose of the Fourth Amendment lays exclusively in the protection of US persons against arbitrary action by government officials and not in restricting acts of governmental agencies towards foreigners.[226] Such an interpretation however clearly contravenes the approach under EU law to consider data protection a universally applicable human right and also the scope of the GDPR which applies regardless of the nationality of the data subject[227] as well as the general prohibition of any discrimination based on nationality in Article 21 CFR. Using different standards for data transfers and data disclosure based on nationality would not thus be in accordance with EU law. Besides, a differentiation between different nationalities would essentially require providers to retain additional personal data of their users in order to ensure, that the data requested by the LEA in fact relates to a non-US person.[228]

4.6. Interim conclusion

It follows that also a bilateral agreement strictly based on the conditions in the CLOUD Act would not serve as a solution for the conflict between the SCA and the GDPR that has been demonstrated, given that the disclosure obligations under the SCA, that may require a provider subject to the GDPR to transfer personal data to the US, would essentially remain unchanged. Rather, such an agreement would only introduce new cross-border production orders between the US and the EU that are however furthermore limited to non-citizens and non-permanent residents of the state where the provider is based. Moreover, the EU and its Member States would be required to remove or at least adapt the limitations on data transfers to third countries under Article 48 in order to allow providers subject to the GDPR to transfer personal data pursuant to a production order by a US LEA. This would not only lower the current standard for data transfers to third countries significantly but essentially contradict the very reason behind including Article 48 in the GDPR.

4.7. A possible way forward

Despite the interim conclusion, a bilateral agreement if not strictly based on the conditions in the CLOUD Act may still serve as a solution. To this end it must not only encompass cross-border production orders in a narrow sense but all production orders that trigger the transfer of personal data out of the protection of the GDPR to the US and regardless of the nationality of the user. Since a US LEA issuing the production order is generally unaware whether the requested information requires the transfer of personal data which is protected under the GDPR, a solution could be achieved by amending the statutory right of the US provider to object to a production order due to a conflict of laws that has been already explicated in Section 2.6.

Accordingly, where the provider demonstrates that disclosing the information sought by the US LEA would conflict with its obligations under the GDPR a potential bilateral agreement could envisage that the US LEA is required to request the personal data concerned based on its powers laid down in the bilateral agreement, instead of

[226] United States v. Verdugo-Urquidez (n 62) 266
[227] Recital 14 GDPR
[228] Mitchol Dunham, 'Arbitrary and outdated: Reforming the Stored Communications Act' (2018), 32 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258774> accessed 20 May 2019

leaving the final decision on how to proceed with the competent US court. Whether it is necessary to curtail the function of the US courts in this context depends on how they will interpret the limitations on data transfers in the scope of the comity analysis. Especially if courts would consider Article 48 as a mere 'blocking statute' it is likely that it would not be accepted as a justification to oppose the disclosure and order the LEA to seek the information by using alternative ways, such as the bilateral agreement or an MLAT.[229]

As regards the first scenario that has been explicated in Chapter 3, involving an EU subsidiary of a US-based provider, the US LEA would have to address a production order based on the agreement directly to the subsidiary. The latter could use the agreement or its implementation under domestic law as the legal basis for transferring the data pursuant to Article 6(1)(c) GDPR. Besides, in case the agreement fulfils the threshold stipulated by both the GDPR and the CJEU, the transfer would also be in accordance with Article 48 GDPR. These arguments would be equally valid for a US-based provider that falls under the scope of the GDPR. Yet, and as has been concluded in Chapter 3, initial guidance by the EDPB on whether compelled disclosure by such a provider constitutes a data transfer should be the first step in this regard.

This seems appropriate also considering that in this scenario all actors are located on US territory and the conflict is only provoked by the extraterritorial reach of the GDPR. Only then and if necessary, can the conditions for such disclosure of personal data to US LEAs be laid down in an agreement as well. Essentially this conflict boils down to the question whether all requirements of the GDPR can be upheld also towards companies based in third countries that nevertheless fall under the scope of the GDPR.[230] The alternative would however be that data subjects using services by such providers would enjoy a significant lower level of data protection which contradicts the intention behind the broad territorial scope of the GDPR to create an equal level of protection to data subjects in the EU, notwithstanding the location of the company processing their data.[231]

From a data protection perspective, the location of the data can be abandoned as the guiding principle to establish jurisdiction in such an agreement. Already under current data protection law, and as has been demonstrated by virtue of the territorial scope of the GDPR, the location of the processing activities is not relevant.[232] Besides it evidently seems obsolete in the age of cloud computing where even single files may be split up and stored on servers in different locations.[233] As has been proven in Section 2.7.2.1., overriding the location of the data as the prevailing principle under international criminal law hitherto by expressive terms in an international agreement would be permissible. Essentially this should exclude such cases from the agreement where the data sought by the LEA is merely stored in one or more data centres in different countries for economic reasons, but where the provider that obtained the production order still acts as the controller or processor in relation to these data.

[229] Kessler, Nowak, Khan (n 171) 609
[230] Svantesson (n 183) 233
[231] European Data Protection Board (n 12) 3
[232] European Data Protection Board 'Opinion on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)' 23/2018 8
[233] Orin Kerr, 'The Next Generation Communications Privacy Act' (2014) 162 University of Pennsylvania Law Review 373, 408

4.8. Feasibility of a bilateral agreement

Prima facie it may appear highly implausible that the US would be willing to commit itself to an agreement that would substantially curtail some of the rights just recently clarified under the CLOUD Act. Already in 2013 *Rauhofer* and *Bowden* have recognized that the US will not consider it unlawful to order the disclosure of user data from companies established and operating in their jurisdiction.[234] Eventually, the commitment by the US will significantly depend on the severity with which the rules on data transfers to third countries will be enforced by European Data Protection Authorities in the discussed cases. However, and in order to avoid putting providers in the middle of the conflict, clear guidance by the EDPB or the competent DPA must first be issued in order to allow the provider to act in accordance with the law.

Furthermore, if adopted in the current form, the EU Regulation on 'European Production and Preservation Orders for Electronic Evidence in Criminal Matters'[235] would require US-based providers which offer services in the EU to respond as well to production orders by European LEAs, irrespective of a bilateral agreement.[236] Such providers moreover would need to appoint a legal representative in the EU against whom the disclosure obligations can be enforced or must otherwise stop offering their services in the EU.[237] Hence, these US-based providers would as well be caught in between conflicting legal obligations as disclosure of content data to foreign governments outside a bilateral agreement continues to be prohibited under US law. The desire for a common solution may thus grow in the US as well. The bilateral agreement would in that case have to be used likewise by European LEAs when ordering data from US-based providers that claim a conflict with US law.

4.9. Essential aspects of a bilateral agreement

In the following, the most essential aspects that have to be addressed in a bilateral agreement between the EU and the US will be assessed which should ensure a fair balance between enhancing access to electronic evidence and the protection of the fundamental right to data protection and privacy.[238] Given the strong ambiguities regarding the scenario involving exclusively a LEA and provider based in the US, the respective discussions are based primarily on the premise that a US LEA would address a production order to a provider established in the EU and subject to the GDPR. Nevertheless, in essence these findings would likewise be applicable if the second scenario is included in the agreement as well.

The conditions stipulated in 18 U.S.C. § 2523(b)(4)(D) can serve as a baseline for the parameters the US government would be willing to apply to its own orders under such a bilateral agreement. This follows from the reciprocity of rights which requires US LEAs to comply with the agreement's procedural and substantive requirements

---

[234] Rauhofer, Bowden (n 63) 26

[235] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters' COM (2018) 225 final (hereinafter 'E-Evidence proposal')

[236] Article 1 (1) E-Evidence proposal

[237] Commission, 'Proposal for a Directive of the European Parliament and the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM (2018) 226 final Article 3(2)

[238] European Data Protection Supervisor (n 219) 9

when requesting data from foreign providers as has been underlined in the results of the ad-hoc group on Cross Border Data Requests.[239]

4.9.1. Conditions for issuing a production order

In order to ensure, that the fundamental rights of the person affected by a production order based on an envisaged bilateral agreement are not compromised, clear conditions for issuing such an order must be determined. The CLOUD Act provides only limited references in this regard and requires first and foremost any production order based on a bilateral agreement to be in accordance with the national law of the issuing LEA.[240] Given that it has been repeatedly held that US domestic law does not provide an adequate level of data protection as EU law, this requirement must however be assessed in more detail.[241]

Since the conditions for issuing a production order often depend on the concerned data category as will be shown below, it is first of all essential to include a clear definition of the data categories encompassed by the agreement which should go beyond a mere differentiation between content and non-content data that is used throughout the proposal for a negotiating directive by the EU-Commission[242] and must concur with the general distinction between subscriber information, metadata and content data under EU law.[243] Moreover, the definitions should be sufficiently precise in order to avoid any overlaps of data categories such as for instance regarding IP-addresses.[244]

4.9.1.1. Prior judicial review

Although not harmonised on an EU-level, the requirement of prior judicial review of production orders concerning certain categories of personal data derives both from the Commission's E-Evidence proposal and the case-law of the CJEU and the ECtHR. According to the E-Evidence proposal, cross-border production orders for content as well as transactional data[245] have to either be issued by a court or validated by it, whereas for access data and subscriber information also the order or validation by the competent prosecutor is sufficient.[246] In those Member States, in which hitherto access to all user data was only permitted subject to prior review by a court, this however would lead to a lowering of the standard which has been criticized.[247] Both the ECtHR and the CJEU on the other hand in their case-law on access to communication data require prior review by a court or another independent authority for both content and metadata,[248] whereas at least the ECtHR expresses a clear preference for a judge.[249]

[239] Krishnamurthy (n 206) 11
[240] 18. U.S.C. § 2523(b)(4)(D)(iii)
[241] Bignami (n 57)
[242] Commission (n 214)
[243] European Data Protection Supervisor (n 219) 15
[244] European Data Protection Board (n 232) 12
[245] The proposal introduces a differentiation of communication meta-data into access data and transactional data.
[246] Article 4(1)(2) E-Evidence proposal
[247] European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Working Document on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters - Introduction and overall assessment of issues' (2018) 2018/0108 (COD) 5
[248] European Data Protection Board (n 232) 14
[249] *Szabo v Hungary* App no 37138/14 (ECtHR 12 January 2016) para 77

According to the CLOUD Act, any production order based on a bilateral agreement 'shall be subject to review or oversight by a court, judge, magistrate, or other independent authority.'[250] Although on first glance this seems in accordance with the requirements under EU law it is not apparent from this wording, whether the review must be conducted *prior* to the issuance of the production order to the provider, which however is an essential requirement that follows from the case-law of the ECtHR and CJEU. To include a clarification in this respect in the agreement is thus essential, in particular considering that under US law, production orders for subscriber information as well as session metadata, which particularly includes the IP-address and time and duration of an access session, can be based on an administrative subpoena, which can be issued directly by a LEA and does not require the prior involvement of a judicial authority.[251]

4.9.1.2. Necessity and proportionality

When issuing a production order, a LEA must be able to demonstrate that there is enough reason to justify this interference with the user's fundamental rights.[252] This should ensure the principle of proportionality and necessity of the measure which has been already recognized in the Preamble to the EU-US Umbrella Agreement[253], that establishes minimum safeguards for the transfer of personal data between the EU and the US for law enforcement purposes, and which is furthermore included in the E-Evidence proposal.[254] In relation to communication data the CJEU has furthermore stated that in order to limit any disclosure to what is strictly necessary and proportionate for the purpose pursued, the law which permits LEAs to order the disclosure of personal data needs to define clearly the circumstances and conditions for such orders and require a link between the requested data and the claimed purpose.[255]

Turning again to the conditions in the CLOUD Act, any order pursuant to a bilateral agreement must be based on 'reasonable justification based on articulable and credible facts, particularity, legality and severity regarding the conduct under investigation'.[256] This standard has been criticised in the US as a vague term not yet defined under US law and thus allowing a broad interpretation by LEAs, which potentially undermines the existing probable cause standard for search and seizure of communication content.[257] Others, such as *Daskal* have held that there is no reason to assume, that the standard for a production order based on a bilateral agreement would be any less than under the SCA.[258]

---

[250] 18 U.S.C. § 2523(b)(4)(D)(v)
[251] Kerr (n 56) 1219
[252] Article 29 Data Protection Working Party (n 156)
[253] Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L 336/3
[254] Article 5(5)(i) E-Evidence proposal
[255] Joined Cases C-203/15 and C-698/15 *Tele 2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson* [2016] ECLI:EU:C:2016:970 para 119
[256] 18. U.S.C. § 2523(b)(4)(D)(iv)
[257] Sabrina A. Morris, 'Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party' (2018) 42 Fordham International Law Journal 183, 215; Lisa V. Zivkovic, 'The Alignment between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject' (2018) 28 Transnational Law & Contemporary Problems 189, 195
[258] Daskal (n 62) 12

Hence, the bilateral agreement needs to further clarify which conditions must be fulfilled by a LEA in order to ensure that only such personal data is transferred which is strictly necessary and proportionate and to prevent any bulk transfers of data. This requires a further limitation which provides that only data of the concrete suspect may be transferred and only in exceptional cases, such as where a concrete threat for national security exists, also data of other people may be included if it can be demonstrated that such data is necessary for the prosecution.[259] Such a limitation is of particular importance as regards data for which under US law an administrative subpoena is sufficient, requiring merely 'relevance' of the data for an on-going investigation, which facilitates ordering data related to a person other than the suspect.

Besides, due to the differentiations between US and non-US persons under current US law, the agreement must determine that the same standard is applicable to all people affected by a production order without discrimination of any kind, especially nationality.[260] It is noteworthy, such an approach has already been foreseen in a bill that should have amended ECPA but did not yet pass the US Congress.[261] This law intends to clarify that the legal standard for accessing content data is probable cause, even when ordering content data of foreigners stored abroad.[262]

Finally, a clear provision on usage limitation is necessary in order to avoid that the strict conditions for obtaining the data get undermined as well as to prevent extensive sharing of data between LEAs and intelligence agencies and the inclusion of the data in general-purpose data bases as it is regularly the case in the US.[263] A respective provision has been already included in the EU-US MLAT, which however leaves broad room for LEAs to use the requested data for purposes not necessarily connected to the initial request.[264] The EU-US Umbrella Agreement can serve as a baseline in this regard, which already requires that personal data is not further processed for purposes incompatible with the purpose for which it was transferred[265] thereby resembling the general requirements for LEAs under EU law.[266]

4.9.1.3. Criminal offence threshold

Another essential aspect in order to ensure proportionality and necessity is to limit production orders to the prosecution of specific crimes. According to the CLOUD Act, a production order shall only be valid for the purpose of obtaining information related to serious crimes.[267] Yet, 'serious crime' is not defined in the SCA itself which leaves some ambiguity with this limitation. When comparing the definitions of the term in

[259] *Tele 2 Sverige* (n 255) 119
[260] Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world* (Council of Europe 2014) 92
[261] International Communications Privacy Act, S. 1671, 115th Cong. (2017)
[262] Zivkovic (n 257) 227
[263] Bignami (n 57) 36; Franziska Boehm, 'A comparison between US and EU data protection legislation for law enforcement purposes' (Policy Department C of the Directorate General for Internal Policies-European Parliament, 2015) 69
[264] Els De Busser, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities*' (Maklu Publishers 2009) 358
[265] Article 6(2) UA
[266] Article 4(1)(b) LED
[267] 18 U.S.C. § 2523(b)(4)(D)(i) SCA

other parts of US statutory law it appears however that it mainly refers to felonies.[268] These are defined as every offense which entails at least a one-year prison-sentence.[269]

In its case-law on data retention and law enforcement access to communication data the CJEU has as well held that access to personal data retained by a provider should be limited to the prosecution of 'serious crimes', where such data may reveal precise details of the affected person's private life, without however providing a clear crime threshold.[270] In its E-Evidence proposal, the Commission partly takes account of the differentiation by the CJEU, by limiting access to transactional data and content data to the prosecution of crimes that entail at least a maximum three-years sentence.[271]

In order to be in accordance with EU law, also production orders by US LEAs, at least those concerning content data and transactional data, must thus be limited to the prosecution of criminal offences that entail a minimum three-year sentence. Considering the differences in criminal law between the EU and US it however would be preferable to attach an annex that exhaustively lists crimes for which production orders based on the bilateral agreement can be issued and the respective data categories that can be requested. Such a list could moreover better safeguard the requirement of dual criminality, which essentially requires that a crime is punishable in both countries, thereby preventing that providers must disclose user data for the prosecution of a conduct that is not punishable under their national law.

In addition it must be recalled that the provisions of the GDPR, insofar as they govern the processing of personal data, must be interpreted in light of all fundamental rights of the CFR,[272] which includes a strict abolition of the death penalty.[273] As a consequence, transfer of personal data for the prosecution of crimes which could lead to death penalty must be excluded.[274] Considering that death penalty under US federal law is foreseen for the most serious crimes including terrorism, this limitation would thus add a cap to the threshold of crimes for which US LEAs can request personal data based on the agreement and would require them to continue using the MLAT procedure or other forms of cooperation for obtaining such data.

4.9.2. Data subject rights and effective judicial remedies

As regards the provision of data subject's rights and effective judicial remedies, according to the EU Commission the Umbrella Agreement should serve as the baseline,[275] which already establishes the rights to access and rectification vis-à-vis competent authorities of the other party and obliges both parties to provide administrative and judicial remedies.[276] The US has implemented the Umbrella Agreement in the scope of the US Judicial Redress Act, which extended certain rights of the US Privacy Act[277] to EU citizens.[278] Following a strict implementation of the

[268] E.g. 22 USC § 4304b(a)(3), 37 CFR § 11.1
[269] 18 USC § 3559
[270] *Tele 2 Sverige* (n 255) 115
[271] Article 5(4) E-Evidence proposal
[272] Joined Case C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk* [2003] ECR I-04989 para 68
[273] Charter of Fundamental Rights of the European Union (n 125) Article 2(2)
[274] Commission (n 214) 11
[275] ibid 6
[276] See Umbrella Agreement Article 16-19
[277] Privacy Act of 1974, Pub.L. 93-579, 88 Stat. 1896 (31 December 1974)
[278] 5 U.S.C. § 552a note

provisions in Article 19 Umbrella Agreement, the US has however refrained from aligning US persons and non-US persons altogether under the Privacy Act and maintained the two-track system in US Privacy Law.[279]

Besides this limitation it must be emphasised that whereas under EU law the provision of data subject's rights and effective judicial remedies originate directly from the fundamental rights of the affected person and any limitations therefore must be necessary and proportionate,[280] the rights and obligations under the Privacy Act can be extensively limited in particular in the law enforcement context, allowing even for the general exclusion of certain law enforcement authorities from the scope.[281] Even under a full alignment with the rights of US citizens under the Privacy Act it remains thus questionable whether this corresponds to an equal level of protection as under EU law.[282]

Hence, although using the Umbrella Agreement as a baseline is welcome from a data protection perspective since it already provides data subject rights to EU citizens, it is apparent that significant changes in US law are still required. In particular it must be ensured that all LEAs that can issue a production order under the bilateral agreement are also obliged to provide access and rectification rights to affected individuals which may only be restricted on a case-by-case basis where necessary and proportionate. Furthermore, judicial remedies must be available in all cases where the rights of the individual are violated which is a prerequisite that must be fulfilled when transferring personal data to third countries.[283] No LEAs may thus be excluded from the scope on a general basis.

4.9.3. User notification

A precondition to allow affected individuals to exercise their rights and apply for remedies is their notification, as they are usually unaware that their personal data has been disclosed to a US LEA. On a general basis, both the provider in relation to the data transfer and the LEA when processing the data are obliged to provide information to the affected person under EU law.[284] However, in order to safeguard amongst others the prevention, investigation and prosecution of criminal offences these rights can be limited.[285] Yet, it follows from the case-law of both the CJEU and the ECtHR that notification should be provided as soon as it would no longer jeopardises on-going investigations.[286]

Under US law LEAs must apply for a 'gag-order' if they want to prevent providers from informing their users about the disclosure of their data. In the application for such an order the LEA must demonstrate that the notification would jeopardise an on-going investigation or endanger the life or physical safety of an individual.[287] Besides, LEAs

[279] Anna Dimitrova, Maja Brkan, 'Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair' (2018) 56 Journal of Common Market Studies 751, 756
[280] See Article 15 LED; Article 16(4) LED;
[281] Bignami (n 57) 35; Boehm (n 263) 55, 69
[282] Boehm (n 263) 70
[283] *Schrems* (n 20) para 64
[284] Article 14(4) GDPR and Article 13(1)(2) LED
[285] Article 23 GDPR, Article 13(3)(b) LED; See also Article 11(2) E-Evidence Proposal
[286] *Zakharov v Russia* App no 47143/06 (ECtHR 22 October 2009) para 234; *Tele 2 Sverige* (n 255) para 121; Opinion 1/15 (n 179) para 220
[287] 18 U.S.C § 2705(b)

are obliged to notify the affected person independently when using an administrative subpoena or a 'd-order'. Thus under US law, notification of the user is the default setting, which is also apparent from the information provided by several of the largest US providers, which only refrain from informing their users if LEAs require it.[288] The bilateral agreement should follow this approach and allow user notification as the default setting unless the issuing LEA explicitly states in the production order that the provider must refrain from informing its user.

Indeed, such an approach would contradict recent developments on a European level, where the Council of the European Union in its General Approach to the E-Evidence proposal has turned this requirement into the opposite by allowing user notification only when explicitly requested by the LEA.[289] Yet, given that it is unpredictable whether US LEAs would be willing and able to inform European users about the disclosure of their data and considering that the provider in general is in a much better position to contact its users, such a requirement clearly would contribute to allow the affected individual to exercise her rights.

4.9.4. Notification of the affected Member State and role of the ISP

In order to safeguard the rights of the affected individual in the context of cross-border production orders it is indispensable that also judicial authorities in the affected Member State are involved in the process. This is necessary since it is predictable that LEAs of the issuing state will usually prioritize their own interests over those of another state and their citizens.[290] Already in the negotiations concerning the E-Evidence proposal on an EU level this aspect has triggered discussions. Essentially, the EU-Commission considered that due to a high level of 'mutual trust' no involvement of other authorities should be necessary. The negotiating process in the Council has however clearly demonstrated that this trust does not exist on an intra-European level, which has led to the introduction of a limited notification obligation when content data is sought and the issuing authority has reason the believe that the affected person does not reside on its territory.[291]

Considering the even greater differences between EU and US law and the stressed relationship as regards data protection especially after the Snowden revelations, it can be assumed, that such trust currently does not exist between the US and all Member States. Notification of a judicial authority in the affected Member States as early as possible therefor is indispensable at least where content data is sought.[292] It has been proposed that notification of the Member State of the residence of the suspect would be

---

[288] See for instance Microsoft 'Data Law - Our practices, principles and policies' <https://blogs.microsoft.com/datalaw/our-practices/>; Google 'Legal process for user data requests FAQs' <https://support.google.com/transparencyreport/answer/7381738?hl=en> accessed 20 May 2019; For a general comparison see Rainey Reitman, 'Who Has Your Back? Government Data Requests 2017' (*Electronic Frontier Foundation*, 10 July 2017) <https://www.eff.org/de/node/96732#govt-requests> accessed 20 May 2019

[289] Council of the European Union, 'Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach' (2018) 15292/18 Article 11(1)

[290] Théodore Christakis, 'E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead' (*Cross-border Data Forum*, 14 January 2019) <https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/> accessed 20 May 2019

[291] Council General Approach (n 289) Article 7a

[292] European Data Protection Supervisor (n 219) 11

the most feasible solution, that would not only ensure safeguarding data protection but also criminal suspect's rights.[293] In case the place of residency of the suspect cannot be determined, no notification should be necessary.[294] In order to avoid delays, such notification would imply a tacit confirmation of the concerned authority where it does not react in a certain time-frame.[295]

The provider on the other hand should only have a limited role. Beside its right to object under the CLOUD Act, a provider should not be required to act as a guarantor for safeguarding fundamental rights. Whereas it should be permitted that companies challenge orders based on formal reasons, a substantive fundamental rights analysis lays outside the abilities of corporations, in particular SMEs.[296]

4.10. Conclusion

Despite the fact that access to electronic evidence might be best solved on an international level, and considering that the recent approaches under the UN framework and the Council of Europe provide promising first results, it appears that in the near term a bilateral agreement between the EU and the US would be the most suitable approach on resolving the conflict between the SCA and the GDPR outside the MLAT procedure. To this end such an agreement must guarantee an equal level of data protection as under EU law. If solely based on the requirements of the CLOUD Act it has been found that an agreement could not be regarded as satisfying this criterion, notably because it would essentially require the EU and its Member States to abolish the limitations on data transfer under Article 48.

In order to serve as a solution, such an agreement must be applicable to all production orders that have a cross-border context. Besides, it needs to include conditions and safeguards that ensure that the rights of the affected user do not get undermined when data is transferred according to the agreement. The most essential aspects to be addressed are the conditions for issuing a production order based on the agreement, including prior judicial review, proportionality and necessity and defining a criminal offence threshold. Moreover, the rights of the data subject and the provision of effective remedies must be ensured, which will require an amendment of the US Judicial Redress Act. In order to facilitate the data subject to exercise her rights, user notification by the provider should be the default setting unless otherwise requested by the issuing LEA. Finally, it is indispensable to include a notification requirement of the affected Member State.

[293] European Data Protection Board (n 232) 16; Théodore Christakis '"Big Divergence of Opinions" on E-Evidence in the EU Council: A Proposal in Order to Disentangle the Notification Knot' (*Cross-border Data Forum*, 22 October 2018) <https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/?cn-reloaded=1> accessed 20 May 2019

[294] Christakis (n 290)

[295] ibid

[296] European Data Protection Supervisor (n 219) 10

Conclusion

By stipulating the doctrine of 'possession, custody and control' of data as the guiding principle for disclosure obligations of providers under the SCA, regardless of the data's location, the CLOUD Act has provided a unilateral answer to safeguard US LEAs access to user data held by providers of electronic communication services and remote computing services such as webmail, instant messaging or social media websites. This approach has been justified with the 'un-territoriality' of data and the fact that LEAs would otherwise be significantly impeded in fulfilling their duties. Indeed, given the business models of several providers, it appears questionable whether the location of the data as being physically encoded into a server still constitutes an appropriate criterion for determining jurisdiction.

Nonetheless, this thesis has demonstrated, that the *opinio iuris* among the state community continues to regard such measures as improper extraterritorial enforcement acts. In particular, the Cybercrime Convention, which hitherto remains the most significant international treaty concerning law enforcement in cyberspace provides no legal basis for such extraterritorial measures. A guidance note on the interpretation of production orders for subscriber information under Article 18 has however opened discussions given that it neglects the data location as the guiding principle and even permits production orders to foreign providers under limited conditions. Yet, as a soft-law measure such an interpretation does not unfold any binding effect on the partying states. Therefor it appears that in absence of any new legal developments, MLATs continue to be the correct form to request data both stored abroad and held by a company on foreign territory.

Regardless of the concerns about the conformity of the disclosure obligations in the SCA with international law, these are nonetheless binding for all providers that fall under US jurisdiction and affect also their subsidiaries on foreign territory, including the EU. This puts such companies in a difficult position since those subsidiaries are bound as well by the GDPR's limitations on data transfers to third countries. The territorial scope of the GDPR on the other hand equally entails extraterritorial effects, obliging also providers solely established on US territory. In essence, the approaches under both the GDPR and the SCA are clear examples of lawmaker's attempts to establish jurisdiction over online services, regardless of traditional territorial boundaries.

Unfortunately, the European data protection framework still lacks a clear definition of a data transfer to a third country. Following the intention behind the rules on data transfer provided in the Regulation itself, it can be contemplated that the rules concern every transfer of personal data by a controller or processor subject to the GDPR to a controller not subject to the GDPR in a third country, regardless of whether the controller or processor initiating the transfer is physically situated on EU territory. The conflict between the SCA and the GDPR can thus be summarized as twofold, triggered both by the extraterritorial effect of the GDPR and the SCA. Where a subsidiary of a US-based provider acts as the controller of the data required by a US LEA, this company must transfer the respective data to its headquarter on US territory insofar as the head office has the legal right to obtain this information from its subsidiary. On the other hand, based on the extraterritorial reach of the GDPR, also a provider on US territory may be obliged to transfer personal data out of the protection of the GDPR to a US LEA.

This thesis has found that a data transfer pursuant to a production order by a US LEA does not fulfil the necessary two-step test as there is neither a legitimate basis for

the processing activity nor are the conditions for data transfers to third countries fulfilled. In particular it clearly contravenes Article 48 of the Regulation which has been drafted in view of limiting the scope of foreign production orders that ignore established channels of international cooperation.

Whereas this conflict could be resolved by either amending the SCA or the GDPR, or by reducing the need for extraterritorial enforcement measures by substantially evolving the MLAT procedure, this thesis has focused on the possibility of an international agreement between the EU and the US as a solution. Based on the global reach of the Internet, access to electronic evidence will eventually need to be resolved on an international level that involves as many countries as possible. Otherwise the tendency to strict data localization requirements may increase further which would undoubtedly threaten the openness of the Internet as such. Yet, despite first efforts both on a UN level and at the Council of Europe, the specific conflict between the SCA and the GDPR cannot be resolved therein for the moment.

The CLOUD Act provides requirements a foreign government must fulfil in order to get into a bilateral data sharing agreement with the US and furthermore includes conditions for direct cross-border production orders to providers. These conditions however do not affect the scope of productions orders under the SCA. Additionally, foreign governments would be obliged to remove any legal barriers that keep providers on their territory from responding to valid US production orders, including such with an extraterritorial effect. Since this would entail the removal of the current restrictions on data transfers to third countries pursuant to foreign production orders under the GDPR, a solution based strictly on the CLOUD Act principles must be declined from a data protection perspective.

Rather, in order to serve as a solution, it must be ensured that all production orders with an extraterritorial effect that require the transfer of personal data out of the protection of the GDPR are included. Yet, as regards data transfers by a controller that falls under the extraterritorial scope of the GDPR, due to existing ambiguities, further guidance by the EDPB or the legislator should be conducted first. In order to reconcile the obligations under the SCA and the GDPR, this thesis has proposed a framework for cross-border production orders which obliges LEAs to make use of the agreement when a provider raises a conflict with foreign data protection rules. Such an agreement would need to include conditions and safeguards that ensure that the rights of the affected user do not get undermined when data is transferred according to the agreement. From a data protection perspective, the following recommendations should thus be considered when drafting a bilateral agreement:

- The data categories which are encompassed by the agreement should be clearly defined in order to provide legal certainty and clarity.
- Judicial review must be conducted prior to the issuance of the production order to the provider.
- Proportionality and necessity must be ensured amongst others by a strict usage limitation and a criminal offence threshold.
- The US Judicial Redress Act must be amended in order to prevent that the far-reaching carve-outs under the US Privacy Act undermine the rights of the data subject as well as the provision of effective judicial remedies.
- User notification by the provider should be the default setting.

- Notification of the Member State of where the affected person has its residence is indispensable.

Finally, the question remains whether from a data protection perspective it is appropriate, in order to reconcile the disclosure obligations under the SCA with the GDPR, to introduce new cross-border production orders which presumably will increase the number of data transfers to US LEAs. Even with the suggested safeguards in place, arguably this will put personal data of people in the EU at a higher risk since the rules of the GDPR can be best enforced when data is held by a controller subject to the GDPR. Nonetheless and as has been illustrated, currently data transfers out of the protection of the GDPR occur without any safeguards in place and global providers will continue to be caught in between two contradicting legal frameworks. Without a bilateral agreement in place or a significant improvement of the MLAT procedure, that re-establishes its attractiveness for LEAs, this situation will remain which puts companies in a constant struggle, undermines data subject's rights and potentially even impedes transatlantic cooperation in criminal prosecutions.

Bibliography

Primary sources

Legislation

European Union Law

Agreement on mutual legal assistance between the European Union and the United States of America [2003] OJ L18/34

Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences [2016] OJ L 336/3

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Charter of Fundamental Rights of the European Union [2012] OJ C326/391

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters [2014] OJ L130/1

Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) [2016] OJ L119/1

Directive (EU) 2016/680 of the European Parliament and of the Council 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] OJ L119/89

Legislative proposals by the European Commission

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, Explanatory memorandum' COM (2018) 225 final

Commission, 'Proposal for a Directive of the European Parliament and the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings' COM (2018) 226 final

Commission, ‘Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters’ COM (2019) 70 final

Commission, ‘Recommendation for a Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185) COM (2019) 71 final

US Statutory Law

Privacy Act of 1974, Pub.L. 93-579, 88 Stat. 1896 (31 December 1974)

Electronic Communications Privacy Act, Pub.L. 99-508, 100 Stat. 1848 (21 October 1986)

Clarifying Lawful Overseas Use of Data Act, Pub.L. 115-141, 132 Stat. 348 (23 March 2018)

International treaties

Council of Europe, ‘Convention on Cybercrime’ (2001) CETS No. 185

Council of Europe, ‘Explanatory Report to the Convention on Cybercrime’ (2001) CETS No. 185

United Nations, ‘Vienna Convention on the Law of Treaties’ United Nations Treaty Series, 1155/331

Case law

Court of Justice of the European Union

Joined Case C-465/00, C-138/01 and C-139/01 *Rechnungshof v Österreichischer Rundfunk* [2003] ECR I-04989

Case C-101/01 *Criminal proceedings against Bodil Lindqvist* [2003] ECR I-12971

Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] ECLI:EU:C:2014:317

Case C-230/14 *Weltimmo v Nemzeti Adatvédelmi és Információszabadság Hatóság* [2015] ECLI:EU:C:2015:639

Case C-362/14 *Maximilian Schrems v Data Protection Commissioner* [2016] ECLI:EU:C:2015:650

Opinion 1/15 [2016] ECLI:EU:C:2017:592

Joined Cases C-203/15 and C-698/15 *Tele 2 Sverige AB v Post- och telestyrelsen* and *Secretary of State for the Home Department v Tom Watson* [2016] ECLI:EU:C:2016:970

Case T-670/16 *Digital Rights Ireland v Privacy Shield* [2017] ECLI:EU:T:2017:838

European Court of Human Rights

Szabo v Hungary App no 37138/14 (ECtHR 12 January 2016)

Zakharov v Russia App no 47143/06 (ECtHR 22 October 2009)

Supreme Court of the United States

United States v. Verdugo-Urquidez, 494 U.S. 259

United States v. Microsoft Corp., 584 U.S. ___

Other US case law

In re Bankers Trust, 61 F.3d 465, 469 (6th Cir. 1995)

United States v. Weaver 636 F.Supp.2d 769 (C.D. Ill. 2009)

United States v. Warshak, 631 F.3d 266, 268 (6th Cir. 2010)

Crispin v. Christian Audigier, Inc., 17 F.Supp.2d 965 (C.D. Cal. 2010)

In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014)

Microsoft Corp. v. United States, 829 F.3d 197, 202 (2d Cir. 2016)

In re Search Warrant No. 16-960-M-01 232 to Google, 232 F. Supp. 3d 708 (E.D.Pa. 2017)

Secondary sources

Official EU documents

European Commission

Commission, 'Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC' SWD (2017) 5 final

Commission, 'Technical Document: Measures to improve cross-border access to electronic evidence for criminal investigations following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace' COM (2017) 9554/17

Council of the European Union

Council of the European Union, 'Outcome report, Seminar on the application of the Mutual Legal Assistance and extradition agreements between the European union and the United States of America' (2016) 9519/16

Council of the European Union, 'Progress Report following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace' (2016) 15072/1/16

Council of the European Union, 'Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters - general approach' (2018) 15292/18

European Parliament

European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)

European Parliament, Committee on Civil Liberties, Justice and Home Affairs '4th Working paper on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters – Relation with third country law' (2019) 2018/0108 (COD)

European Parliament Committee on Civil Liberties, Justice and Home Affairs, 'Working Document on the Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters - Introduction and overall assessment of issues' (2018) 2018/0108 (COD)

Article 29 Data Protection Working Party

Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' WP128

Article 29 Data Protection Working Party, 'Opinion 05/2012 on Cloud Computing' WP 196

Article 29 Data Protection Working Party, 'Comments on the issue of direct access by third countries' law enforcement authorities to data stored in other jurisdiction, as proposed in the draft elements for an additional protocol to the Budapest Convention on Cybercrime' (2013)

Article 29 Data Protection Working Party, 'Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' WP 217

Article 29 Data Protection Working Party, ‘Statement on Data protection and privacy aspects of cross-border access to electronic evidence’ (2017)

European Data Protection Board

European Data Protection Board, ‘Guidelines on derogations of Article 49 under Regulation 2016/679’ (2018) 2/2018

European Data Protection Board, ‘Guidelines on the territorial scope of the GDPR (Article 3) - Version for public consultation’ (2018) 3/2018

European Data Protection Board, ‘Opinion on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)’ 23/2018

European Data Protection Supervisor

European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe”’ (2012)

European Data Protection Supervisor, ‘Opinion of the European Data Protection Supervisor on the data protection reform package’ (2012)

European Data Protection Supervisor, ‘Opinion on the negotiating mandate of an EU-US agreement on cross-border access to electronic evidence’ 2/2019

Official US policy documents

Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the U.S. Senate (15 July 2016)

Mulligan S, ‘Cross-Border Data Sharing Under the CLOUD Act’ Congressional Research Service Report prepared for Members and Committees of US Congress’ (2018)

United States Department of Justice, ‘Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act’ (Whitepaper 2019)

Council of Europe

Council of Europe Cybercrime Convention Committee (T-CY) ‘Ad-hoc Sub-Group on Transborder Access to Data and Jurisdiction: Terms of Reference (adopted at the 6th Plenary)’ (2011) T-CY (2011)05

Council of Europe Cybercrime Convention Committee (T-CY) 'Transborder access and jurisdiction: What are the options? Report of the Transborder Group' (2012) T-CY (2012)3

Council of Europe Cybercrime Convention Committee (T-CY) 'Draft elements of an Additional Protocol to the Budapest Convention' (2013) T-CY (2013)14

Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note # 3 Transborder access to data (Article 32)' (2014) T-CY (2013)7

Council of Europe Cybercrime Convention Committee (T-CY) 'Transborder access to data and jurisdiction: Options for further action by the T-CY Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction' (2014) T-CY (2014)16

Council of Europe Cybercrime Convention Committee (T-CY) 'Criminal justice access to data in the cloud: challenges' (2015) T-CY (2015)10

Council of Europe Cybercrime Convention Committee (T-CY) 'Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY' Final report of the T-CY Cloud Evidence Group (2016) T-CY (2016)5

Council of Europe Cybercrime Convention Committee (T-CY) 'Summary report of the 1st Meeting of the T-CY Protocol Drafting Plenary' (2017) T-CY (2017)38

Council of Europe Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note#10 Production orders for subscriber information (Article 18 Budapest Convention)' (2017) T-CY (2015)16

Council of Europe Cybercrime Convention Committee (T-CY) 'Provisional draft text of provisions: Languages of requests, Emergency MLA, Video conferencing' (2018) T-CY (2018)23

United Nations

United Nations Special Rapporteur on the right to privacy, 'Annual Report 2018' A/HRC/37/62

UNODC, *Comprehensive Study on Cybercrime, Draft – February 2013* (United Nations New York, 2013)

UNODC, *Practical Guide for Requesting Electronic Evidence Across Borders* (United Nations Vienna, 2019)

Amici curiae

Brief of the European Commission on behalf of the European Union as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

Brief of Amici Curiae Fourth Amendment Scholar, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

Brief of Jan Philipp Albrecht, Sophie in 't Veld, Viviane Reding, Birgit Sippel, and Axel Voss, Members of the European Parliament as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

Brief of EU Data Protection and Privacy Scholars as Amici Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

Brief of U.N. Special Rapporteur on the Right to Privacy as Amicus Curiae, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016)

Books

Colonna L, 'Europe Versus Facebook: An Imbroglio of EU Data Protection Issues' in Gutwirth, Leenes, De Hert (eds), *Data Protection on the Move. Law, Governance and Technology Series, vol 24* (Springer, Dordrecht 2015)

Council of Europe Commissioner for Human Rights, *The rule of law on the Internet and in the wider digital world* (Council of Europe 2014)

Daskal J, Vladeck S, 'Incidental Foreign Surveillance and the Fourth Amendment' in Gray, Henderson (eds), *The Cambridge Handbook of Surveillance Law* (Cambridge University Press 2017)

De Busser E, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities* (Maklu Publishers 2009)

European Union Agency for Fundamental Rights (FRA), *Handbook on European data protection law* (2nd edn Publications Office of the European Union 2018)

Kerr O, *Computer Crime Law* (4th edn, American Case Book Series 2018)

Kleijssen J, Perri P, 'Cybercrime, Evidence and Territoriality: Issues and Options' in Kuijer, Werner (eds), *Netherlands Yearbook of International Law 2016* (Springer 2016)

Schweighofer E, 'Principles for US-EU Data Flow Arrangements' in Svantesson, Kloza (eds), *Trans-atlantic data privacy relations as a challenge for democracy* (Intersentia 2017)

Velasco C, Hörnle J, Osula A, 'Global Views on Internet Jurisdiction and Trans-border Access' in Gutwirth, Leenes, De Hert (eds), *Data Protection on the Move. Law, Governance and Technology Series, vol 24*, (Springer, Dordrecht 2016)

Voigt P, Von dem Bussche A, *The EU General Data Protection Regulation – A practical guide* (Springer 2017)

Walden I, 'Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent' in Pearson, Yee (eds), *Privacy and Security for Cloud Computing* (Springer, 2012)

Wall D, 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing', in

Brownsword, Scotford, Yeung (eds), *The Oxford Handbook on the Law and Regulation of Technology* (Oxford University Press 2017)

Articles

Balboni P, Pelino E, ‘Law Enforcement Agencies' activities in the cloud environment: a European legal perspective’ (2013) 22 Information & Communications Technology Law

Bilgic S, ‘Something old, something new, and something moot: The Privacy Crisis under the CLOUD ACT’ (2018) 32 Harvard Journal of Law & Technology

Brkan M, Dimitrova A, ‘Balancing National Security and Data Protection: The Role of EU and US Policy-Makers and Courts before and after the NSA Affair’ (2018) 56 Journal of Common Market Studies

Colonna L, ‘Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?’ (2014) 4 International Data Privacy Law

Currie R, ‘Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is the Microsoft Ireland Case the «Next Frontier»?’ (2017) 54 The Canadian Yearbook of International Law

Daskal J, ‘The Un-Territoriality of Data’ (2015) 125 Yale Law Journal

Daskal J, ‘Borders and Bits’ (2018) 71 Vanderbilt Law Review

Daskal J, ‘Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0’ (2018) 71 Stanford Law Review

Daskal J, ‘Unpacking the CLOUD Act’ (2019) 4 Eucrim The European Criminal Law Associations Forum

De Hert P, Czerniawski M, ‘Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context’ 6 International Data Privacy Law (2016)

De Hert P, Parlar C, Sajfert J, The Cybercrime Convention Committee’s 2017 Guidance Note on Production Orders: Unilateralist transborder access to electronic evidence promoted via soft law’ (2018) 34 Computer Law & Security Review

De Hert P, Parlar C, Thumfart J, ‘Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders’ (2018) 9 New Journal of European Criminal Law

De Hert P, Thumfart J, ‘The Microsoft Ireland case and the cyber- space sovereignty trilemma. Post-territorial technologies and companies question territorial state sovereignty and regulatory state monopolies’ (2018) 4 Brussels Privacy Hub Working Paper

Galbraith J, ‘Contemporary practice of the United States relating to international law’ (2018) 112 American Journal of International Law 490

Gimelstein S, ‘A location-based test for jurisdiction over data: The Consequences for global online privacy’ (2018) 1 University of Illinois Journal of Law, Technology & Policy

Kerr O, ‘A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it’ (2004) 72 George Washington Law Review

Kerr O, ‘The Next Generation Communications Privacy Act’ (2014) 162 University of Pennsylvania Law Review

Kessler D, Nowak J, Khan S, ‘The potential Impact of Article 48 of the General Data Protection Regulation on cross border discovery from the US’ (2016) 17 Sedona Conference Journal

Krishnamurthy V, ‘Cloudy with a conflict of laws’ (2016) The Berkman Center for Internet & Society at Harvard University Research Publication No. 2016-3

Koops B, Goodwin M, ‘Cyberspace, the Cloud, and Cross-Border Criminal Investigation the Limits and Possibilities of International Law’ (2016) 5 Tilburg Law School Legal Research Papers Series

Morris S, ‘Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party’ (2018) 42 Fordham International Law Journal

Rauhofer J, Bowden C, ‘Protecting their own: Fundamental rights implications for EU data sovereignty in the cloud’ (2013) University of Edinburgh School of Law Research Paper Series No 2013/28

Schwartz P, ‘Information Privacy in the Cloud’ (2013) 161 University of Pennsylvania Law Review

Seitz N, ‘Transborder Search: A new perspective in law enforcement?’ (2005) 7 Yale Journal of Law and Technology

Svantesson D, ‘The regulation of cross-border data flows’ (2011) 3 International Data Privacy Law

Svantesson D, ‘Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation’ (2015) 5 International Data Privacy Law

Svantesson D, ‘European Union Claims of Jurisdiction over the Internet – an Analysis of Three Recent Key Developments’ (2018) 9 Journal of Intellectual Property, Information Technology and Electronic Commerce Law (JIPITEC)

Zivkovic L, ‘The Alignment between the Electronic Communications Privacy Act and the European Union's General Data Protection Regulation: Reform Needs to Protect the Data Subject’ (2018) 28 Transnational Law & Contemporary Problems

Legal studies

Bignami F, ‘The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens’ (Policy Department C of the Directorate General for Internal Policies-European Parliament, 2015)

Boehm F, ‘A comparison between US and EU data protection legislation for law enforcement purposes’ (Policy Department C of the Directorate General for Internal Policies-European Parliament, 2015)

Online sources

AccessNow, ‘Mutual Legal Assistance Treaties – Country Profile United States’ <https://www.mlat.info/country-profile/united-states> accessed 20 May 2019

Blair T, Lawler T, ‘Possession, Custody or Control: A Perennial Question Gets More Complicated’ *The Legal Intelligencer* (Philadelphia, 5 February 2018) <https://www.law.com/thelegalintelligencer/sites/thelegalintelligencer/2018/02/05/possession-custody-or-control-a-perennial-question-gets-more-complicated/> accessed 20 May 2019

Christakis T, ‘”Big Divergence of Opinions” on E-Evidence in the EU Council: A Proposal in Order to Disentangle the Notification Knot’ (*Cross-Border Data Forum*, 22 October 2018) < https://www.crossborderdataforum.org/big-divergence-of-opinions-on-e-evidence-in-the-eu-council-a-proposal-in-order-to-disentangle-the-notification-knot/?cn-reloaded=1> accessed 20 May 2019

Christakis T, ‘Lost in the Cloud? Law Enforcement Cross-border Access to Data After the “Clarifying Lawful Overseas Use of Data” (CLOUD) Act and E-Evidence’ (*FIC Observatory*, 28 June 2018) <https://observatoire-fic.com/en/lost-in-the-cloud-law-enforcement-cross-border-access-to-data-after-the-clarifying-lawful-overseas-use-of-data-cloud-act-and-e-evidence/> accessed 20 May 2019

Christakis T, ‘E-Evidence in a Nutshell: Developments in 2018, Relations with the Cloud Act and the Bumpy Road Ahead’ (*Cross-border Data Forum*, 14 January 2019) < https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/> accessed 20 May 2019

Colangelo A, Parrish A, ‘International Law and Extraterritoriality: Brief of International and Extraterritorial Law Scholars as Amici Curiae (U.S. v. Microsoft)’ (2018) SMU Dedman School of Law Legal Studies Research Paper No. 382 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3105491> accessed 20 May 2019

Council of Bars and Law Societies of Europe (CCBE) ‘Position on the Commission proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters’ (2018) <https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20181019_CCBE-position-on-Commission-proposal-Regulation-on-European-Production-and-Preservation-Orders-for-e-evidence.pdf> accessed 20 May 2019

Daskal J, Woods A, ‘Cross-Border Data Requests: A Proposed Framework’ (*Lawfare*, 24 February 2015) <https://www.lawfareblog.com/cross-border-data-requests-proposed-framework> accessed 20 May 2019

Daskal J, ‘Access to Data Across Borders: The Critical Role for Congress to Play Now’ (*American Constitution Society for Law and Policy*, 24 October 2017)

<https://www.acslaw.org/issue_brief/briefs-landing/access-to-data-across-borders-the-critical-role-for-congress-to-play-now/> accessed 20 May 2019

Daskal J, Swire P, 'A possible US-EU Agreement on Law Enforcement Acces to Data?' (*Just Security*, 21 May 2018) <https://www.justsecurity.org/56527/eu-agreement-law-enforcement-access-data> accessed 20 May 2019

Dunham M, 'Arbitrary and outdated: Reforming the Stored Communications Act' (2018) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258774> accessed 20 May 2019

Information Commissioner's Office 'Guide to Data Protection – International transfers' <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/> accessed 20 May 2019

Kent G, 'Sharing Investigation-Specific Data with Law Enforcement: An International Approach' (2014) Stanford Public Law Working Paper <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2472413> accessed 20 May 2019

Korff D, 'Key points re the Cybercrime Convention Committee (T-CY) Report: Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group T-CY (2016)5' (2016) <https://edri.org/files/surveillance/korff_note_coereport_leaaccesstocloud%20data_final.pdf> accessed 20 May 2019

Lackey M, Pottinger O, 'Stored Communications Act: Practical Considerations' (*LexisNexis*, 22 June 2018) <https://www.lexisnexis.com/lexis-practice-advisor/the-journal/b/lpa/archive/2018/06/22/stored-communications-act-practical-considerations.aspx> accessed 20 May 2019

Loeb R, 'The CLOUD Act Explained' (*Orrick*, 6 April 2018) <https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained> accessed 20 May 2019

Reitman R, 'Who Has Your Back? Government Data Requests 2017' (*Electronic Frontier Foundation*, 10 July 2017) <https://www.eff.org/de/node/96732#govt-requests> accessed 20 May 2019

Smith D, 'ICO Brings Some Welcome Clarification to the GDPR's International Transfer Rules' (*Allen & Overy Digital Hub*, 7 September 2018) <http://aodigitalhub.com/2018/09/07/ico-brings-some-welcome-clarification-to-the-gdprs-international-transfer-rules/> accessed 20 May 2019