HARVARD LAW SCHOOL | The Case Studies

CSP060
APRIL 2020

CLOUD Act Enforcement

RYAN CHAN-WEI AND SEBASTIAN STEUER

Memorandum

DATE: February 18, 2020
TO: Junior Attorneys, Terrorist Financing Task Force
FROM: William Parr, Vice-Chair, Terrorist Financing Task Force
RE: Pursuing enforcement actions under the U.S. CLOUD Act

In one of our most important terrorist finance investigations, we have run into a complex transatlantic data privacy issue involving FinTech customer data stored on a cloud server in Europe. We have a series of urgent meetings with key stakeholders scheduled for next week, and our new Chair would like to be briefed on these matters by the end of this week.

As some of you may know, the [redacted] recently foiled an attempted terrorist attack on [redacted], and subsequent investigations revealed that the operation was partly funded by [redacted]. Early investigative leads have revealed that the mastermind behind the attack was [redacted], working in conjunction with the European branch of the [redacted] terrorist organization. One major figure in the planning and financing of the attack might be [redacted], a Swiss citizen currently believed to live in a suburb of Zurich.

However, the investigation into the financier has hit a significant roadblock because we have trouble accessing his financial records. The money has most likely been channeled to the attackers through the financier's account with [redacted], a Paris-based FinTech company specializing in international payments services. Obviously, we would like to get access to these financial records as soon as possible to proceed with our investigation. Unfortunately, the FinTech company is very proud of its privacy policies and it is very unlikely that it would be willing to cooperate on a voluntary basis.

Written by Ryan Chan-Wei and Sebastian Steuer under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

A traditional method of getting access to the data would be to rely on mutual legal assistance of our European colleagues under the applicable mutual legal assistance treaties ("MLAT").[1] However, these procedures have often proven inflexible and slow. There is also a high risk that the length of the MLAT process may result in a leak of the investigation to the suspect, which would allow them to evade arrest.

This is why we are currently exploring a different option. We discovered that the FinTech company is a heavy user of remote computing services and stores all of its customer data "in the cloud." Specifically, they employ the services of [redacted], one of the largest U.S.-based internet companies. [redacted] stores the data on servers close to its customers and, in this case, all the data we need is stored on servers in France.

Our aim now is not to get the data from the FinTech company, but from the cloud computing provider. We are aware that the general Department practice is to reach out to the enterprise directly and to avoid asking cloud service providers for enterprise customer data. However, after long discussions with the legal team, we have concluded that the requirements are met for an exception under the relevant Department policies.[2] The U.S. Attorney's Office for the Southern District of New York was eventually able to obtain a warrant issued under the Stored Communications Act ("SCA") as amended by the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act")[3]. Using the powers under the CLOUD Act would allow us, in principle, to sidestep the MLAT process. However, our CLOUD Act approach is not free of problems either and, due to strict European data protection rules, there is now a severe transatlantic conflict of data privacy laws.

As you may have heard, the European Union's approach to privacy and data protection differs fundamentally from the U.S. approach. On the one hand, the field of information privacy law in the U.S. is essentially a patchwork of constitutional and statutory provisions. These rules often address specific and rather narrow aspects of privacy, or set out data protection standards only for certain industries. On the other hand, the European framework is much more uniform and holistic. Another important conceptual difference is that in the U.S., the processing of personal data is generally allowed unless there is a specific law that restricts such processing. The European thinking, by contrast, starts from the notion that every individual has a constitutionally protected right to privacy and data protection that prohibits the collection and processing of personal data. The processing is only lawful if a specific law allows it.

In this case, because both the FinTech company and the cloud service provider have a physical presence in the E.U., the data also falls within the scope of the European General Data Protection Regulation[4] ("GDPR"). Among other things, this regulation sets out tough restrictions for data transfers to third countries (*i.e.*, data transfers to entities located outside of the E.U.). Therefore, from the perspective of European law, the cloud provider cannot easily produce the data stored on its European servers to the U.S. government, because it is obligated to observe the strict GDPR requirements for data transfers to third countries. While going through an MLAT generally satisfies the GDPR transfer requirements, it is very difficult to execute a transfer directly from the provider to the U.S. government without any involvement of E.U. or E.U. Member State authorities.

---

[1] See Agreement on Mutual Legal Assistance, E.U.–U.S., Jun. 25, 2003, T.I.A.S. No. 10-201.1; see also Instrument as contemplated by Article 3, paragraph 2, of the Agreement on Mutual Legal Assistance between the United States of America and the European Union signed 25 June 2003, as to the application of the Treaty on Mutual Legal Assistance in Criminal Matters Between United States of America and France signed 10 December 1998, Fr.–U.S., Jun. 25, 2003, T.I.A.S. No. 10-201.32.

[2] *See* DOJ, *Seeking Enterprise Customer Data Held by Cloud Service Providers* (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download.

[3] Stored Communications Act,18 U.S.C. Chapter 2701, *et seq.*, as amended by the Cloud Act, Pub.L. 115–141 (which also amended the Electronic Communications Privacy Act, 18 U.S.C. 2510, *et seq.*).

[4] Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

From the perspective of U.S. law, however, it does not matter where the data is stored. The SCA only requires that the internet company qualifies as a remote computing service provider pursuant to the relevant definition,[5] and that the data is within the provider's "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[6] Thus, we are in a situation where U.S. law potentially demands that the provider violate GDPR transfer provisions by handing over data stored in the E.U. to U.S. authorities.

To refresh your memory of the CLOUD Act, I have attached as Annex A a note circulated by Julia from the Office of Policy and Legislation last year after the Department published its White Paper. For a more detailed introduction, you may also want to refer to the White Paper itself, which is included in the Appendices. Additionally, I have also attached as Annex B a note prepared by Jack giving an overview of the relevant GDPR provisions. For a more detailed overview of the "different visions of data privacy" on the opposite sides of the Atlantic, you may also wish to refer to the appended Georgetown Law Journal article by *Schwartz* and *Pfeifer*.[7]

Unfortunately, this current case only represents the tip of the iceberg. As the investigation progresses, it is inevitable that more essential information will be uncovered, and it is highly probable that the process of obtaining that information will give rise to further data privacy issues and conflicts with the GDPR. Furthermore, in light of the increasingly cross-jurisdictional nature of terrorist funding, similar cases are likely to emerge again soon. Given the manifold ways of storing and encrypting data in the cloud, we will likely be confronted with even more complex problems soon. Future cases may include complications such as non-U.S. based cloud providers, data shards, and data trusts.

Lastly, encryption is another topic that we should keep in mind. This is not a pressing issue at the moment because the cloud provider in this case should be able to give us access to the unencrypted data. However, the CLOUD Act is explicitly "encryption-neutral" and does not require providers to be capable of decrypting their data. Thus, it is highly likely that a case will eventually arise where we obtain a warrant for cloud-stored data only to find out that the data has been encrypted and the cloud-storage provider is not in possession of the keys necessary to decrypt the data. Such encrypted data would pose a severe impediment to law enforcement efforts because the commonly used ciphers cannot be cracked even with the entire computing power of our government. This may change once we have powerful quantum computers, but unfortunately this will still take quite a while, notwithstanding recent advances in that field of technology. Until then, we have to be aware of the limits that encryption sets on our ability to access the global cloud even with the geographically broad access that the CLOUD Act gives us.

It is therefore essential for us to have a deep understanding of these issues and a clear policy on how to deal with the CLOUD Act, especially in relation to data stored in the E.U.. To that end, a meeting is scheduled next week with our new Chair and several key stakeholder groups to explore future steps. In preparation for that meeting, it will be your job to brief the Chair on some of the key issues that will likely be discussed.

Introduction

To get everybody on the same page, we should start the briefing with a quick introduction to the CLOUD Act. The Chair should be briefed on the developments that led to the need for a "clarification" of the

[5] 18 U.S.C. § 2711(2).
[6] 18 U.S.C. § 2713.
[7] Paul M. Schwartz and Karl-Nikolaus Pfeifer, *Transatlantic Data Privacy Law*, 106 GEO. L. J. 115 (2017).

extraterritorial reach of SCA warrants, namely the *Microsoft*[8] case, and the purposes that Congress pursued in passing the CLOUD Act. Specifically, the brief should explain why the traditional MLAT process is no longer appropriate in today's highly digitalized and globalized world, and why the CLOUD Act helps law enforcement adapt to the times. Furthermore, the introduction should quickly sketch the main features of the CLOUD Act, highlighting in particular the providers' options to file a motion to quash a warrant. The brief should also address the significance of the so-called "qualifying foreign governments" ("QFG").

The main part of the briefing should then be structured around some specific issues that will likely be brought up by the stakeholder groups. In the remainder of this memorandum, I will call your attention to what I believe are the main issues that should be discussed with the relevant stakeholder groups.

European Data Protection Representatives

The Chair will be meeting with public stakeholders that have an interest in the observance of the GDPR. This includes officials from the European Commission, the European Data Protection Board ("EDPB"), the European Data Protection Supervisor ("EDPS"), and the French Data Protection Authority (the Commission Nationale de l'Informatique et des Libertés, or "CNIL"). The Chair will need to be briefed on the European perspective in this case, namely how the conflict between the CLOUD Act and the GDPR might be resolved, and if it is at all possible to do so.

Unfortunately, at the moment it appears that service providers are caught between a rock and a hard place, because complying with a warrant issued under the CLOUD Act invariably leads to them violating the GDPR. The Chair needs to be briefed on how the Europeans interpret the GDPR provisions regarding data transfers out of the E.U. (see Annex 2 for an overview of these provisions). It would, of course, be desirable if we can find a way to resolve this conflict without the need to enter into any new agreements. I suspect that the officially published communications by the EDPB will take a particularly strict stance on the GDPR's data transfer provisions, and advocate for a very narrow interpretation of any exceptions. However, in practice it is the Member States authorities who make the decisions. In our experience, when it comes to granting exceptions, they often tend to be a bit more flexible than one would expect from a literal reading of the official guidelines. This is especially true for time-sensitive terrorism cases, where bureaucratic blockades of data transfers might have particularly dire consequences.

Another possible way out of this dilemma would be if the U.S. were to enter into an executive agreement with the E.U. or individual Member States, recognizing them as a "qualifying foreign government." The existence of an executive agreement might legalize the data transfer under GDPR rules. Even if this was not the case, the executive agreement would open up an avenue by which the CLOUD Act warrant could be quashed or modified (as long as the suspect is neither a United States citizen nor resident in the United States) under the CLOUD Act's specific comity analysis. An executive agreement should also be to the benefit of the E.U. and its Member States. Due to the worldwide operations of the big U.S. tech companies, we receive myriad MLAT requests every year ourselves, including from Europe. An executive agreement would allow law enforcement authorities in E.U. Member States to request data directly from U.S. service providers.

Looking to the future, the Chair also needs to be briefed about the likelihood that transatlantic agreement can be reached on evidence-sharing in criminal procedures and the current state of negotiations.

[8] *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016). In this case, Microsoft successfully challenged a subpoena for data stored on an Irish server. The case was appealed and heard by the Supreme Court, and judgment was vacated and the case remanded with instructions to dismiss the case as moot after the passage of the CLOUD Act, *see United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

Notwithstanding some differences in the scope of privacy regulation, we have always been able to find common ground for cooperation in the past. Frankly, I would be surprised if the Europeans fundamentally disagreed with the underlying approach of the CLOUD Act. After all, they currently have a proposal pending for an e-Evidence Directive that bears much similarity to the CLOUD Act and, to me, this suggests that the E.U. and the U.S. are generally on the same page concerning the need for reform to adapt to the increasingly digital world in which we now live.

Privacy Advocates

The Chair will also be meeting with stakeholders who resolutely oppose the CLOUD Act, such as the Open Technology Institute, the American Civil Liberties Union, and the Electronic Frontier Foundation. She needs to be briefed on the rationale behind their opposition to the CLOUD Act, and whether those positions can be reconciled with those of the Act's proponents.

The privacy concerns with respect to the U.S. government seeking access to data stored abroad are not necessarily the same as those with respect to qualified foreign governments seeking access to data stored with providers subject to U.S. jurisdiction. To this end, it might be advisable to differentiate between the different parts of the CLOUD Act.

Those who criticize the CLOUD Act for failing to adequately protect human rights often focus on the part of the Act that enables qualified foreign governments to access data without going through the MLAT process. Their key argument is that the Act's human rights and privacy safeguards are not sufficiently rigorous and might therefore threaten the privacy of U.S. citizens whose data can be accessed by foreign governments without any significant involvement from U.S. courts or authorities. In this respect, it is essential to have a clear picture of exactly which aspects of the Act are being criticized by the privacy and human rights advocates.

The Chair will presumably also discuss the encryption problem with these stakeholders.[9] Under the existing legislation, there is virtually nothing we can do to require providers to be capable of decrypting cloud-stored data. They are free to set up their systems so that only the customer has access to the keys necessary to decrypt the stored data, and potentially frustrate any attempt of the government to access the data through the provider. Unsurprisingly, privacy supporters are quite happy with the status quo. On the other hand, the Department has repeatedly urged Congress to adopt laws requiring communication providers to be able to decrypt any customer data (sometimes referred to as "backdoor" policies).

The Attorney General recently reheated this debate in an emphatic speech. Proponents, including our Department leadership, tend to argue that absent backdoor laws, terrorists and criminals can use encryption to operate completely in the dark. As a result, the government would no longer be able to effectively protect national security and the lives of American people. In response, most counterarguments question the technical feasibility of "backdoors," and express concern over the privacy risks that they would inevitably introduce. We certainly do not need to go into all the details and many dimensions of this debate in preparation for the meeting, but it would be helpful if you could briefly summarize the chief arguments on both sides.

[9] Other teams within the Department have already done substantial work on encryption-related issues. Therefore, we have requested if a member of these teams could participate in the meeting to give a quick summary presentation. In this case, you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

Cloud Computing Providers

The Chair will be meeting with representatives of the leading global cloud computing providers (*e.g.*, Google, Amazon, and Microsoft), all of whom are based in the United States. It is important for us to maintain a functioning working level relationship with these providers.

The Chair is interested in understanding their opinions on the CLOUD Act, and if there are any differences between them. Microsoft, for example, is usually mentioned as a *supporter* of the CLOUD Act. This is not self-explanatory given the non-trivial conflict that a CLOUD Act warrant may put them in (*i.e.*, forcing them to violate either the order of the United States government or the GDPR). Furthermore, internet companies usually claim that they have a strong interest in keeping their customers' data private. Therefore, it would be interesting to know what factors drive their support of the CLOUD Act.

Another set of issues that the Chair wishes to discuss with the cloud providers relates to the different technical models by which data can be stored in the cloud, namely data localization models (where the data is stored on one server in a particular country, usually near the customer), data shards (where the data is split up into pieces and stored across many servers in many countries) and data trusts (where the main provider cooperates with a trustee and thus has no immediate access to the data).[10] Presumably, it would be sensible to give the Chair a quick primer on these three models and then analyze if there are any differences as to their treatment under the CLOUD Act. Such differences could potentially exist a) with respect to the question whether the data is in "possession, custody, or control" of the provider, or b) with respect to the comity analysis that has to be carried out if the provider tries to quash the warrant.

FinTech Coalition

The Chair will be meeting with stakeholders from a FinTech coalition, comprising companies both from the U.S. and abroad. They are concerned about how the CLOUD Act will impact their business model, and the Chair needs to be briefed about the potential implications of the Act on the ability of FinTechs to protect data privacy. While our specific case especially attracted the attention of other FinTech companies, keep in mind that the data privacy issues raised by the CLOUD Act are also of broader relevance for the financial industry and cloud computing customers in general.

To obtain a better understanding of the underlying business considerations, the Chair would first like to obtain a quick overview of the increasing relevance of cloud computing in the financial sector, with a focus on why more and more financial companies are outsourcing their IT to cloud computing providers, and on the risks associated with this practice.

Importantly, the Chair should also be briefed on the options that cloud users have to evade the reach of the CLOUD Act and, thus, potentially enhance the privacy protection of their customers' data. Besides the idea of using data trusts (which we will have already discussed with the cloud computing providers), there are two other strategies that should be considered.

First, cloud computing users could try to switch to providers that are not based in the U.S. or enter into storage agreements only with the foreign subsidiaries of U.S.-based providers. Obviously, this only helps

[10] We assume that other teams within the Department already have some experience with the data storage models commonly used by U.S. cloud service providers. As with the encryption issues, we have therefore requested if one of their experts could participate in the meeting to give a quick summary presentation. In this case, you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

if the foreign provider is not subject to the CLOUD Act as well. Thus, some inquiry into the territorial applicability of the CLOUD Act with respect to providers (and not only to their data) might be necessary.

Second, cloud computing customers may think about using encryption and key management options that would prevent the provider from accessing the unencrypted data from the outset.[11] The Chair is certainly not interested in all the technical details but it would be helpful to provide a brief overview of the common options for customers to encrypt their data in the cloud and the implications of these options for government requests.[12] You can assume that all of the three major cloud providers offer, at least on the level of abstraction that is of interest for us, roughly similar encryption options.

Legal Scholars

Finally, the Chair will be meeting with a group of legal scholars who are experts in data protection law and international law. This meeting is particularly important, because she hopes to obtain the validation and buy-in of key academic stakeholders. Support from the legal academy will be essential in structuring our policy positions, given the number of complex legal issues that arise when pursuing enforcement actions under the CLOUD Act. Prior to this meeting, the Chair will need to be briefed on a number of normative questions.

In this context, the Chair should first be briefed on the fundamental ways to think about the meaning of "territoriality" when it comes to data and privacy. If the established categories no longer fit, it is easier to justify why we need to explore new regulatory paths and use innovative mechanisms such as those under the CLOUD Act.

Second, we need to brief the Chair on how requests for data under the CLOUD Act interact with, and possibly even threaten, the sovereignty of another country. This requires some analysis on how we should understand sovereignty in the context of the global cloud. There are no straightforward or easy answers to this question. After all, the interests that states have in exercising authority over and protecting the privacy of the data stored on servers in their territory may vary according to the circumstances of the individual case.

We certainly need not reinvent the wheel in these debates. However, it would be helpful for the Chair to have an overview of the key debates in the academic literature before she meets with some of the leading scholars in the field.

Lastly, as you can see, even though the CLOUD Act has the word "*Clarifying*" in its name, many questions still remain to be answered, and the Act opens up yet another chapter in the decades-long transatlantic struggle over data privacy. I hope that your briefings for the Chair will shed some light on these issues and help us gain a better understanding of how best to respond to the changes brought by the digital cloud.

---

[11] *EBA, Guidelines on Outsourcing (EBA/GL/2019/02)*, Eur. Bkg. Auth. ¶. 68(e) (Feb. 25, 2019), https://eba.europa.eu/documents/10180/2551996/EBA+revised+Guidelines+on+outsourcing+arrangements.pdf/38c80601-f5d7-4855-8ba3-702423665479, Privacy concerns are not the only reason why financial institutions might be interested in encrypting their data. Encryption is also an important building block of general cybersecurity risk management procedures. According to the European Banking Authority, institutions and payment institutions should, when employing cloud computing services, "consider specific measures, where necessary, for data in transit, data in memory and data at rest, such as the use of encryption technologies in combination with an appropriate key management architecture", *see* Deloitte, *Deloitte Note: EBA Guidelines on Outsourcing (EBA/GL/2019/02)*, DELOITTE ¶ 68(e) (Feb. 25, 2019) (summarizing the EBA Guidelines), https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_EBA%20outsourcing%20guidelines.pdf.

[12] As indicated earlier (*supra* note 9), other teams within the Department have already done substantial work on encryption-related issues, and we have requested if one of their experts could participate in the meeting. If this is the case, the expert's presentation will likely also cover encryption key management, and you would not need to include this issue in your brief. Please check with your supervisor if we have received a response from the other teams before you start working on this part of the brief.

Many thanks, and I look forward to seeing everyone later this week.

Annex 1

Note on The CLOUD Act

DATE: April 19, 2019

TO: All Attorneys, Criminal Division

FROM: Julia Ehrenreich, Legal Analyst, Office of Policy and Legislation

RE: U.S. CLOUD Act

You may have already read the Department's White Paper on the CLOUD Act that was published last week, but it may nevertheless be helpful to have a quick internal overview of the underlying purpose of the Act and its key provisions before we use of it in practice.

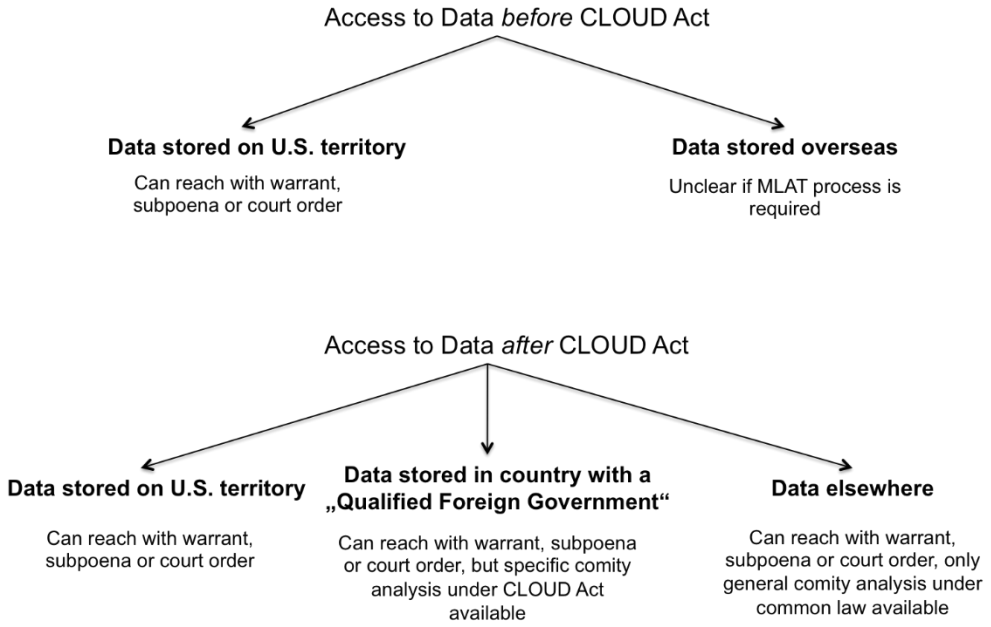
At its core, the CLOUD Act was introduced to "speed access to electronic information held by U.S.-based global providers" because the mutual legal assistance process occasionally proved "too cumbersome" and hindered electronic evidence from being processed in "a timely manner."[1] To this end, the CLOUD Act compels a U.S. service provider to disclose electronic data "regardless of whether such communication, record, or other information is located within or outside the United States."[2]

From an enforcement perspective, this is a powerful tool. It means that only the ability to access the data matters and not the location where the data is actually physically stored. The Act is, therefore, a significant development, because it represents "a first step in what may be a paradigm shift in how access to digitized data is regulated."[3]

Before the passage of the CLOUD Act, it was unclear whether the mere accessibility of data by a U.S. information service provider sufficed to enforce a warrant under the Secured Communications Act (SCA). The following figure illustrates that shift in paradigm:

[1] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, U.S. DEP'T OF JUSTICE 2 (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download.
[2] 18 U.S.C. § 2713 (2018).
[3] Frederick T. Davis and Anna R. Gressel, *Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIGATION 1, 5 (2018), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/fall/storm-clouds-or-silver-linings/, https://www.debevoise.com/insights/publications/2019/02/storm-clouds-or-silver-linings.

Figure 1: Changes Introduced by the CLOUD Act[4]

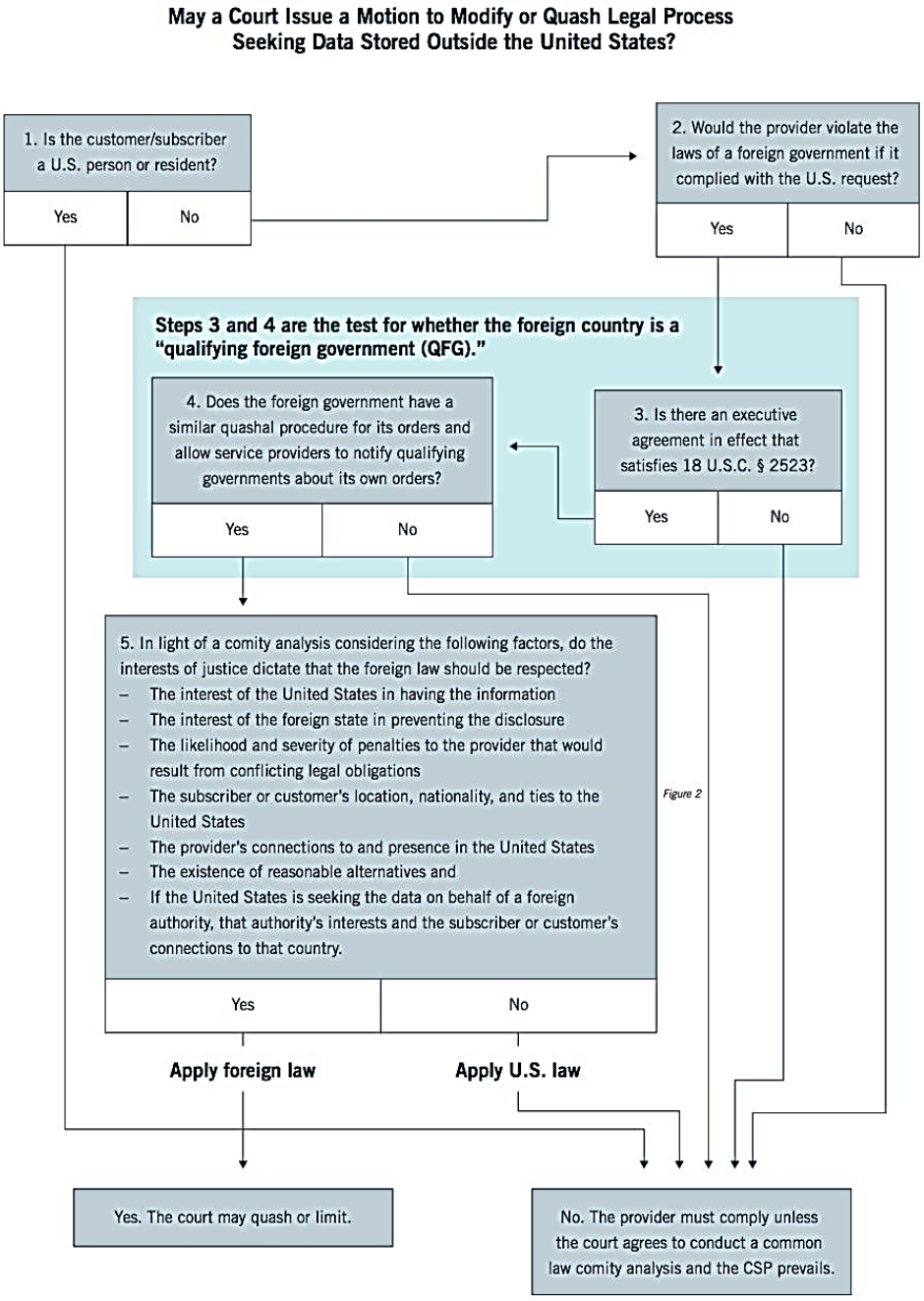


However, the extraterritorial reach of the CLOUD Act naturally gives rise to conflicts of laws and the Act, therefore, also provides for the possibility of quashing (or modifying) a CLOUD Act request if, *inter alia*, compliance with the order would breach the laws of a "qualifying foreign government." Whether the United States recognizes another country's government as a "qualifying foreign government" turns on several safeguards, such as whether the country has "adequate substantive and procedural laws on cybercrime and electronic evidence" and "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government."[5] It is noteworthy that the Act does not preclude courts from quashing the request under a common law comity analysis even when the foreign country does not have a "qualifying foreign government."[6]

The following flowchart, extracted from a Dechert LLP white paper, provides a helpful summary of the new process introduced by the CLOUD Act.[7]

[4] *Id.*; "MLAT" refers to a *mutual legal assistance treaty*, which is a reciprocal agreement between two or more countries to exchange information that aids in the enforcement of criminal law; "belong" refers to "possession, custody, or control" of the data (18 U.S.C. § 2713); the term "United States person" means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States (18 U.S.C. § 2523).
[5] 18 U.S.C. § 2523 (2018).
[6] H.R. 1625, 115th Cong. div. V, § 103(c) (providing a rule of construction for 18 U.S.C. § 2703).
[7] Ben Barnett, Jeffrey A. Brown, Dr. Olaf Fasshauer, Vernon L. Francis and Theodore E. Yale, *Forecasting the Impact of the New US CLOUD Act*, DECHERT (Apr. 2018), https://www.dechert.com/content/dam/dechert%20files/knowledge/publication/2018/4/White%20paper%20-%20Cybersecurity%20-%20Cloud%20Act%20-%2004-18.pdf.

Figure 2: Responding to a CLOUD Act Request[8]



Another key aspect of the CLOUD Act is that it makes it easier for foreign law enforcement agencies to access data held by U.S. providers by allowing QFGs to request data from such providers directly and without going through the MLAT process. Because most of the world's largest internet companies are based in the U.S., the DoJ has to deal with myriad requests by foreign governments under various MLATs. To make this process more efficient, which would be in the interest of both the U.S. and foreign

[8] *Id.*; for the details of what would constitute an executive agreement that satisfies 18 U.S.C. § 2523, see ORIN KERR, COMPUTER CRIME LAW 37-43 (4th ed. Supp. 2018) in the appendix; "CSP" refers to a cloud service provider.

governments, the DoJ had long sought to establish an alternative framework. Notably, this project had started even before the issues pertaining to overseas-stored data attracted considerable attention. The part of the Act dealing with the extraterritorial reach of SCA warrants was added to this project only later, and after the government's defeat in the Second Circuit in the *Microsoft* case.[9]

[9] *Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016). In this case, Microsoft successfully challenged a subpoena for data stored on an Irish server. The case was appealed and heard by the Supreme Court, and judgment was vacated and the case remanded with instructions to dismiss the case as moot after the passage of the CLOUD Act, *see United States v. Microsoft Corp.*, 584 U.S. ___, 138 S. Ct. 1186 (2018).

Annex 2

Note on GDPR Data Transfer Rules

DATE: February 15, 2020
TO: William Parr, Vice-Chair, Terrorist Financing Task Force
FROM: Jack Hoffmann, Junior Analyst, Terrorist Financing Task Force
RE: GDPR Data Transfer Rules

This note provides a brief overview of the data transfer rules under the European Union's General Data Protection Regulation (GDPR).[1] The objective is to lay out the core principles, without going into all the details of this complex body of law.[2]

As the first word of its title suggests, the scope of the *General* Data Protection Regulation is extremely broad. It uses very extensive definitions of "personal data" and "processing" (Article 4(1) and (2) GDPR), and is not limited to automated processes. It applies across industries, and to data processing by both the private and the public sector. It is also important to note that the GDPR does not only protect data subjects located in the European Union. So long as an enterprise has a minimal physical—not necessarily legal—establishment in the Union, GDPR requirements apply to all operations in connection with this establishment, regardless of the location of the data subject (Article 3(1) GDPR).[3] .

Arguably, the most important GDPR provision is Article 6(1), pursuant to which any processing of personal data is only lawful if at least one of six justifications applies. These justifications are consent, contract, compliance with a legal obligation, vital interests of the data subject, carrying out tasks in the public interest, and legitimate interests. It is important to note that as a general matter that the mere existence of legitimate interests does not suffice to justify the processing under the legitimate interests clause; rather, the legitimate interests have to be of such significance that the relevant rights and interests of the data subject do not outweigh them.

According to European doctrine, a data transfer out of the E.U. constitutes a processing in and of itself and must be justified by one of the justifications under Article 6(1). In addition to Article 6(1), Title V of the GDPR (Articles 44 through 50) includes further restrictions with respect to data transfers to third countries. The objective of these restrictions is to ensure that the strict GDPR standards for data

[1] Regulation (E.U.) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[2] One important feature of the GDPR not reflected in this note is the distinction between data controllers and processors. A data controller is any "natural or legal person" . . . which . . . "determines the purposes and means of the processing of personal data" (Art. 4(7) GDPR). A processor is any "natural or legal person" . . . "which processes personal data on behalf of the controller" (Art. 4(8) GDPR). The terminology is somewhat confusing, as both the controller and the processor can "process" data (as defined in Art. 4(2) GDPR). In each case, the limitations discussed in this note apply. If a natural person has an account with a cloud computing provider, the provider would be the processor. If an enterprise stores customer data in the cloud, the enterprise would be the controller and the cloud provider the processor. In general, the processing of data by a processor is subject to additional requirements specified in Art. 28 GDRP, and in particular limited by the processing agreement between the processor and the controller. However, we currently assume that the processing agreements used by the major U.S. cloud providers would allow a data transfer in response to an SCA warrant. Under these circumstances, the distinction between processors and controllers would not matter for purposes of the CLOUD Act.

[3] Absent an establishment in the Union, the GDPR may still apply so long as the E.U. market is targeted, *see* Art. 3(2) GDPR. Only in this case the applicability is limited to data subjects who are located in the Union.

processing cannot simply be undercut by transferring the data from European territory. The penalties imposed for noncompliance with the GDPR are severe. Pursuant to Article 83 of the GDPR, unauthorized "transfers of personal data to a recipient in a third country" can be punished by "administrative fines up to $20 million E.U.R, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher."

According to Article 48 of the GDPR, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognized or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State." Thus far, only the United Kingdom has entered into an agreement with the U.S. regarding the CLOUD Act that may qualify as an agreement under Article 48.[4] Apart from the special case of the UK, there are only traditional MLAT agreements in place between the U.S. and the E.U. and/or its Members States.

In addition to Article 48, Recital 115 of the GDPR makes very clear that the E.U. is not willing to accept the extraterritorial application of third countries' laws absent any agreement. Apparently, European lawmakers already anticipated the situation under CLOUD Act in this recital:

> Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States.
>
> This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.
>
> The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation.
>
> Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met.
>
> This may be the case, inter alia, where disclosure is necessary for an important ground of public interest recognized in Union or Member State law to which the controller is subject.

The only transfer rule that would allow a transfer absent an agreement is Article 49 of the GDPR, which permits derogations for specific circumstances. However, it is not clear if data transfers in response to CLOUD Act requests could be based on this exceptional provision, and it appears more likely than not that the leading authorities will interpret the exceptions very strictly, in line with the strong culture of data privacy in Europe.

[4] See Dep't of Justice, *Press Release: U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, U.S. Dep't of Justice (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists. The agreement is available here: https://tinyurl.com/y5mobx8v.

Appendices

Overview / Introduction (*to be read by all students)

1. CLOUD Act, H.R. 1625, 115th Cong. div. V.

2. Brief for the United States, *United States v. Microsoft*, 138 S. Ct. 356 (2017), vacated and dismissed as moot, 138 S. Ct. 1186 (2018). Summary and Section C of Argument, U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (2019).

3. Frederick Davis & Anna Gressel, *Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act*, 45 LITIGATION 1 (2018).

4. Ben Barnett et al., *Actual Impact of 2018 U.S. CLOUD Act Still Hazy,* LEXOLOGY (July 29, 2019), https://www.lexology.com/library/detail.aspx?g=179b5200-0308-4478-b14f-5e2d027ee058.

5. General Data Protection Regulation (GDPR), Regulation (E.U.) 2016/679 (Apr. 27, 2016). Only the provisions mentioned in the memo and the other annexes need to be considered.

6. *Paul M. Schwartz & Karl-Nikolaus Pfeifer*, Transatlantic Data Privacy Law, 106 GEO. L. J. 115 (2017). Introduction and Section I.

European Data Protection Representatives

7. Council of the European Union, Decision authorizing the opening of negotiations with a view to concluding 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 (May 21, 2019), ST 9114/19 and addendum ST 9666/19.

8. EDPS and EDPB, Initial legal assessment of the impact of the US CLOUD Act on the E.U. legal framework for the protection of personal data and the negotiations of an E.U.-US agreement on cross-border access to electronic evidence, Annex to letter of July 10, 2019 to the Chair of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE).

9. U.S. Dep't of Justice, *Press Release, Joint US-E.U. Statement on Electronic Evidence Sharing Negotiations*, U.S. DEP'T OF JUSTICE (Sept. 26, 2019), https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

10. Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. F. 1029 (2019), Introduction and Section II.B. (1039-1043).

11. European Commission, *Press Release, Fact Sheet and Q&A on e-Evidence Proposals*, EUR. COMM. (Apr. 2018), https://europa.eu/rapid/press-release_IP-18-3343_en.htm.

Privacy Advocates

Privacy issues under the CLOUD Act

12. Neema Singh Guliani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, LAWFARE (Mar. 16, 2018), https://www.lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them.

13. Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L & COMP. L. 57 (2019). Introduction, Section III.A.

14. Secil Bilgic, *Something Old, Something New, and Something Moot: The Privacy Crisis Under the CLOUD Act*, 32 HARV. J.L. & TECH. 321 (2018). Introduction, Sections IV.A. and IV.C.

Encryption

15. Harold Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1(1) JOURNAL OF CYBERSECURITY 69 (2015).

16. Jim Baker, *Rethinking Encryption,* LAWFARE (Oct. 22, 2019), https://www.lawfareblog.com/rethinking-encryption. Sections I and II.

17. Josh Benaloh*, What if Responsible Encryption Back-Doors Were Possible?*, LAWFARE (Nov. 29, 2018), https://www.lawfareblog.com/what-if-responsible-encryption-back-doors-were-possible.

18. William P. Barr, *Keynote Address*, International Conference on Cyber Security, https://justice.gov/opa/speech/attorney-general-william-p-barr-delivers-keynote-address-international-conference-cyber (July 23, 2019).

19. Sally Q. Yates and James B. Comey, *Going Dark: Encryption, Technology, and the Balance between Public Safety and Privacy*, Testimony before the Committee on the Judiciary of the United States Senate (July 8, 2015).

Cloud providers

20. Brad Smith, *The CLOUD Act is an important step forward, but now more steps need to follow*, MICROSOFT (Apr. 3, 2018), https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/.

21. Michael Punke, *AWS and the CLOUD Act*, AWS SECURITY BLOG (May 27, 2019), https://aws.amazon.com/de/blogs/security/aws-and-the-cloud-act/.

22. Google, *Transparency Report: User Data Requests* (2019), https://transparencyreport.google.com/user-data/overview?hl=en.

23. Google, *White Paper Government Requests Google Cloud* (Oct. 2018),Tech Companies Letter of Support for Senate CLOUD Act (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf.

24. Microsoft Press Release, *Microsoft Announces Plans to Offer Cloud Services from German Datacenters* (Nov. 11, 2015), https://news.microsoft.com/europe/2015/11/11/45283/.

25. Microsoft Press Release, *Microsoft to deliver cloud services from new datacenters in Germany in 2019 to meet evolving customer needs* (Aug. 31, 2018), https://news.microsoft.com/europe/2018/08/31/microsoft-to-deliver-cloud-services-from-new-datacentres-in-germany-in-2019-to-meet-evolving-customer-needs/.

26. Paul Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681 (2018). Introduction, Sections I.B. and II.A.2.

FinTech Coalition

27. Hal Scott et al., *Cloud Computing in the Financial Sector: A Global Perspective*, PROGRAM ON INTERNATIONAL FINANCIAL SYSTEMS (Jul. 2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf. Sections 1 and 2.

28. *Google*, Government requests for customer data: controlling access to your data in Google Cloud (June 2019), https://services.google.com/fh/files/blogs/government_access_technical_whitepaper.pdf.

Legal Scholars

29. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015). Introduction, Section II.

30. Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016). Introduction, Section II.

31. Frederick T. Davis, *A U.S. Prosecutor's Access to Data Stored Abroad–Are There Limits?*, 49 INTERNATIONAL LAWYER 1 (2015). Skip Sections I to III.