GT GreenbergTraurig

Memorandum

TO: Dutch Ministry of Justice and Security –NCSC

FROM: Greenberg Traurig LLP | Gretchen Ramos, Andrea Maciejewski and Herald Jongen

DATE: July 26, 2022

RE: Application of the CLOUD Act to EU Entities

You have requested us to advise on the CLOUD Act's applicability to European Union (EU) entities and cloud providers (collectively, EU Entities), and the steps that EU Entities can take to ensure that they are not subject to the CLOUD Act. You have asked the following 6 questions regarding the CLOUD Act, which we will answer below:

1. Please advise whether an EU Entity is within the reach of the CLOUD Act, even if the EU Entity is not located in the United States (U.S.).
2. Please advise whether an EU Entity that is not located in the U.S., but that offers services and products to customers in the U.S., would be subject to the CLOUD Act.
3. Please list other relevant U.S. laws that could impact an EU Entity.
4. Please indicate whether the U.S. can obtain data from an EU Entity, over whom it does not have jurisdiction, by ordering a U.S. national, employed by the EU Entity in Europe, to hand over the EU Entity data by relying on the CLOUD Act or some other law.
5. What happens if a foreign entity with no presence in the U.S., but who has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, ignores a CLOUD Act order?
6. Please advise whether the CLOUD Act extends to all data in the custody, control and possession of an EU Entity, who has no presence in the U.S. but who has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, or only to that data which relates to a U.S. citizen.

Conclusion

EU Entities can be within the reach of the CLOUD Act, even if the EU Entities are located outside the U.S. In order for an EU Entity to completely avoid being subject to the CLOUD Act, it would need to process data using a non-U.S. entity, which either

a) does not have a corporate relation to any company with a presence in the U.S. (such as a U.S. subsidiary) and that does not have sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity/non-US entity (which includes not selling products or services to customers in the US); or
b) if it does have a corporate relationship with a company based in the U.S., the U.S. company must not have possession, custody, or control over the data that is stored in the EU.

In no case can the EU Entity have a U.S. parent company, as the parent would be considered to have possession of or control over the data of its subsidiary

Furthermore, it is advisable not to employ US nationals who have access to relevant data.

Question 1: Please advise whether an EU Entity is within the reach of the CLOUD Act, even if the EU Entity is not located in the United States (U.S.).

Response: Yes, under certain circumstances, an EU Entity, that is a provider of electronic communication service (ECS) or remote computing service (RCS), and not located in the U.S. could still be subject to the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) if the EU Entity has sufficient contacts with the U.S. such that personal jurisdiction can be exercised over the EU Entity. Cloud suppliers qualify as a provider of ECS and/or RCS.

The CLOUD Act is a federal law that has two distinct parts, each of which provides the U.S. government with a unique way to access data held by private companies.[1] The CLOUD Act does not function as a stand-alone law, but instead amends two titles of the existing Electronic Communications Privacy Act (ECPA). Whether an EU Entity that is not located in the U.S. is within the reach of the CLOUD Act will depend on (1) the type of CLOUD Act order, and (2) the specific facts and circumstances. The CLOUD Act does not expand U.S. courts jurisdiction over foreign companies.

Stored Communications Act. The CLOUD Act first amends Title II of ECPA – also known as the Stored Communications Act (SCA).[2] The SCA only regulates access to the content of electronic communications and cloud-stored documents, and non-content data relating to electronic communications (like transmission records and user-account information), but not other types of personal or business data.

The SCA amendment clarifies existing obligations under the SCA by explaining that communication service providers (CSPs) must comply with an order made pursuant to the SCA *regardless* of whether the communication, record, or other information requested is located within or outside of the United States, as long as the information is within the CSPs possession, custody or control[3] The Department of Justice (DOJ) has made it clear that the SCA amendment "does not create any new form of warrant. It simply clarifies the obligations under the Stored Communications Act of providers subject to U.S. jurisdiction, including obligations to disclose information pursuant to warrants."[4]

Whether the U.S. government can obtain data from an EU Entity pursuant to an SCA order, will depend on several factors. First, a warrant may be issued only if the U.S. government demonstrates probable cause that the communications sought will establish

---

[1] *See* DEPARTMENT OF JUSTICE, CLOUD ACT RESOURCES (updated Jan. 2022), last accessed May 20, 2022, available at https://www.justice.gov/dag/cloudact.

[2] CLOUD Act § 103(a) (2018); 18 U.S.C § 2713 (2018).

[3] 18 U.S.C § 2713 (2018) (stating that "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.").

[4] DEPARTMENT OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT, FAQ 18 at pg. 13 (Apr. 2019), available at https://www.justice.gov/dag/page/file/1153436/download [hereinafter CLOUD Act Whitepaper].

evidence of a crime.[5] Second, the U.S. government must either establish the EU Entity had continuous and systematic presence in the U.S. or it must satisfy the "minimum contacts" test to assert jurisdiction over the EU Entity, and where the minimum contacts analysis is close, the U.S. government must establish that the exercise of personal jurisdiction over the EU Entity is not unreasonable.[6] Third, the communications sought must be within the EU Entity's possession, custody or control.

The U.S. government has personal jurisdiction over:

1. A U.S. legal entity;
2. A foreign entity with an office in the U.S. (such as a branch office);[7]
3. A foreign entity in the U.S. who has enough contacts with the U.S. to satisfy the requirements of personal jurisdiction.[8]

As described in more detail, in the response to Question 2, U.S. courts analyze various factors when determining whether personal jurisdiction exists over a foreign entity, including whether the entity is selling its services or products to people or businesses located in the U.S., marketing and advertising in the U.S., and working with U.S. service providers.[9] And for a foreign entity offering its services online, U.S. courts also will analyze whether the foreign entity has an interactive website that is accessible in the U.S., whether they are blocking U.S. IP addresses, and whether the entity is using U.S. based servers.[10] Generally, none of these factors is determinative as to whether personal jurisdiction exists, but rather are viewed together to assess whether the foreign entity availed itself of doing business in the U.S., and thus personal jurisdiction exists.

Even assuming that the U.S. governmental entity is successful in asserting personal jurisdiction, it must also establish the EU Entity is in "possession, custody or control" of the data sought. The CLOUD Act, which does not define what "possession, custody or control" means in relation to electronic data explicitly, is "encryption-neutral" and does not require providers to be capable of decrypting their data. Thus, to the extent the EU Entity Is storing encrypted data, and it is not in possession of the keys necessary to decrypt the data, the EU Entity would not be in a position to determine whether it has data sought by the warrant. Furthermore, in such circumstances, and assuming the technology does not exist to decrypt the data, it may be challenging to establish the EU Entity is, in fact, in possession, custody or control of data that is responsive to the warrant.
Thus, even if an EU Entity is located wholly outside of the U.S., it could still be subject to the CLOUD Act if it has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, and it is in possession, custody or control of the data sought under the warrant. If, however, it is determined that the EU Entity's

[5] *See* 18 U.S.C. § 2703(a) (requiring that any warrant issued under the SCA be "issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction").

[6] *See generally Int'l Shoe Co. v. Wash.*, 326 U.S. 310, 316 (1945).

[7] *See infra* discussion of General Personal Jurisdiction in Question 2; *Perkins v. Benguet Consol. Min. Co.,* 342 U.S. 437, 445 (1952) (the Court held that a foreign corporation had continuously and systematically conducted business in Ohio because the company's president kept company files and held directors' meetings in the Ohio office, carried on correspondence relating to the business in Ohio, distributed salary checks drawn on two active Ohio bank accounts, and engaged an Ohio bank to act as transfer agent.).

[8] *See infra* response to Question 2.

[9] *See Knox v. Metalforming, Inc.,* 914 F.3d 685 (1st Cir. 2019).

[10] *See Plixer Int'l., Inc. v. Scrutinizer GmbH*, 905 F.3d 1, 7 (1st Cir. 2018).

contacts are not enough to establish personal jurisdiction, or if the EU Entity is not in the possession, custody or control of the data sought, then it is not within the reach of the CLOUD Act.

Wiretap Act Amendment. Second, the CLOUD Act amends Title I of ECPA – also, known as the Wiretap Act.[11] The Wiretap Act amendment allows the U.S. government to engage in bi-lateral agreements with foreign countries, which are negotiated by the Executive branch.[12] These agreements are intended to eliminate conflict of law issues, allowing CSPs to disclose electronic data directly to foreign authorities pursuant to covered orders without the use of a mutual legal assistance treaty.[13]

Where the U.S. government is relying on a bi-lateral agreement made pursuant to ECPA to obtain data from an EU Entity, and where the government has obtained a lawful order against the EU Entity, then the EU Entity is directly within the purview of the CLOUD Act, regardless of whether that EU Entity is located in the U.S. or the relevant foreign nation.[14] In 2019, the U.S. and EU met to begin negotiations on electronic evidence sharing, but to date, the U.S. has not entered into a Cloud Act agreement with any EU member state. To date, the U.S. has a Cloud Act agreement in place with the United Kingdom and Australia, and is in discussions with Canada to finalize a Cloud Act agreement.[15]

Question 2: Please advise whether an EU Entity that is not located in the U.S., but that offers services or products to customers in the U.S., would be subject to the CLOUD Act.

For purposes of our response, we assume the CLOUD Act order was made pursuant to the amended SCA rather than pursuant to a Wiretap Act bi-lateral agreement (which, as mentioned above, is not in place with any EU member state).

Response: An EU Entity that is not located in the U.S., but that offers services or products to customers in the U.S., might be subject to the CLOUD ACT (i.e., the SCA) depending on the specific facts.

A U.S. federal law's applicability to a foreign entity depends on whether the foreign entity is subject to U.S. personal jurisdiction.[16] A determination of personal jurisdiction is a highly fact-dependent analysis that looks at whether the company (i) has affiliations with the U.S. that are so continuous and systematic as to render it essentially at home in the U.S.[17] or otherwise (ii) has "certain minimum contacts with [the U.S.] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice.'"[18]

---

[11] CLOUD Act § 103(b) *et seq*. (2018); 18 U.S.C § 2523 (2018).

[12] 18 U.S.C § 2523 (2018).

[13] CLOUD Act Whitepaper 4.

[14] 18 U.S.C. 2523(b) (2018); CLOUD Act Whitepaper 5 ("Orders requesting data must be lawfully obtained under the domestic system of the country seeking the data; must target specific individuals or accounts; must have a reasonable justification based on articulable and credible facts, particularity, legality, and severity; and must be subject to review or oversight by an independent authority, such as a judge or magistrate.").

[15] *See* The United States Department of Justice, Cloud Act Resources at https://www.justice.gov/dag/cloudact, last viewed on May 24, 2022.

[16] *Helicopteros Nacionales de Colombia, S.A. v. Hall*, 466 U.S. 408, 413 (1984).

[17] *Daimler AG v. Bauman*, 571 U.S. 117, 137 (2014).

[18] *International Shoe Co.,* 326 U.S. at 316.

General Personal Jurisdiction: Personal jurisdiction premised on contacts that are so continuous and systematic as to render a company essentially at home in the U.S. is defined as "general personal jurisdiction."[19] General personal jurisdiction focuses on whether a company's contacts with the U.S. are so expansive that the company could be brought to court in the U.S. for *any* claim, regardless of where the claim or harm arose. In other words, general personal jurisdiction determines whether the company itself is subject to U.S. law, rather than whether a company's specific actions are subject to U.S. law.

In determining whether the U.S. has general personal jurisdiction over a company, U.S. courts look at whether the company's actions (including the actions of the company's employees) indicate a continuous and/or systematic trend of activities in the U.S. such that the company should reasonably expect that it could be brought to court in the U.S. In conducting its analysis, the courts may look at, among other things, whether the company is incorporated in the U.S., has active bank accounts in the U.S., whether the company regularly holds business meetings in the U.S., and whether the company maintains files or other physical items in the U.S.[20] Ordinarily, no one action is dispositive of whether the U.S. has general personal jurisdiction over a company. Instead, the courts look at the company's overall business activities in the U.S.

Although whether personal jurisdiction exists and the CLOUD Act applies is determined on a case-by-case basis, typically jurisdiction would be found to exist over an EU Entity, with no presence in the U.S., only if the EU Entity's activities within the U.S. are so continuous that it effectively is fully operational in the U.S.

Specific Personal Jurisdiction: If a court determines that the U.S. does not have general personal jurisdiction over an EU Entity, it will then assess whether the U.S. has "specific personal jurisdiction" over the EU Entity.[21] Unlike general personal jurisdiction, which focuses on whether the company itself should be subject to U.S. law, specific personal jurisdiction looks at whether a specific act or activity relating to the company's contacts with the U.S. should be subject to U.S. law. Put another way, in finding specific personal

---

[19] *Goodyear Dunlop Tires Operations, S.A. v. Brown,* 564 U.S. 915, 924 (2011) ("Adjudicatory authority so grounded is today called 'general jurisdiction.'") (citing *Helicopteros Nacionales de Colombia, S.A.,* 466 U.S. 408).

[20] *Perkins,* 342 U.S. at 445 (the court held that a foreign corporation had continuous and systematic contact with Ohio because the president kept company files and held directors' meetings in the Ohio office, carried on correspondence relating to the business in Ohio, distributed salary checks drawn on two active Ohio bank accounts, and engaged an Ohio bank to act as transfer agent.); *Goodyear Dunlop Tires Operations, S.A.,* 564 U.S. at 924 (noting that the "place of incorporation, and principal place of business [is the] 'paradig[m]' bases for the exercise of general jurisdiction.") (quoting Brilmayer & Paisley, *Personal Jurisdiction and Substantive Legal Relations: Corporations, Conspiracies, and Agency*, 74 Cal. L.Rev. 1, 14, 29–30 (1986)); *Helicopteros Nacionales de Colombia, S.A.,* 466 U.S. at 415 (1984) (the Court held that a foreign company which did not have a place of business in Texas and had never been licensed to do business in Texas, and whose contacts with Texas consisted "of sending its chief executive officer to Houston for a contract-negotiation session; accepting into its New York bank account checks drawn on a Houston bank; purchasing helicopters, equipment, and training services from Bell Helicopter for substantial sums; and sending personnel to Bell's facilities in Fort Worth for training", was not enough to establish general jurisdiction.).

[21] *International Shoe Co.,* 326 U.S. at 318-20 (distinguishing between situations where the Court has jurisdiction over a company due to "continuous and systematic" contacts and situations where the Court has jurisdiction over a company due to the company having "sufficient contacts or ties with the state of the forum to make it reasonable and just according to our traditional concept of fair play and substantial justice to permit the state to enforce the obligations which appellant has incurred there.").

jurisdiction, an EU Entity would only be subject to U.S. law for those harms or actions occurring in the U.S. that relate the EU Entity's business operations in the U.S.[22]

In making a determination of specific personal jurisdiction, the courts look at whether the company has "minimum contacts" or ties with the U.S. such that it would be reasonable to permit the U.S. to exercise jurisdiction over the company.[23] This "minimum contacts" inquiry is broken down into three separate questions:[24]

1. Does the claim arise directly out of, or relate to, the company's activities in the U.S.?[25]
2. Do the company's contacts in the U.S. represent a purposeful availment of the privilege of conducting activities in the U.S., thereby making the company's involuntary presence before U.S. courts foreseeable? [26]
3. Is the exercise of jurisdiction reasonable?[27]

Whether a claim arises out of the company's activities in the U.S. is a fairly straightforward inquiry. There must be "an affiliation between the [U.S.] and the underlying controversy, principally, [an] activity or an occurrence that takes place in the [U.S.] and is therefore subject to [U.S.] regulation."[28] In other words, if the controversy does not relate to an action or harm that occurred within the geographic boundaries of the U.S., then there is no specific personal jurisdiction and the EU Entity would not be subject to the CLOUD Act.

Assuming the harm or controversy occurred in the U.S., the courts will then analyze whether the company has deliberately taken advantage of the benefits and protections of doing business in the U.S., such that the company could reasonably foresee that it would be subject to the U.S. court system.[29] In determining whether a company has purposefully availed itself of U.S. law, the courts focus in part on the company's intentions.[30] An accidental or attenuated connection with the U.S., such as a connection occurring entirely through a third-party actor, will generally not be enough to establish specific personal jurisdiction. [31]

---

[22] *Goodyear Dunlop Tires Operations, S.A.,* 564 U.S. at 924; *Ford Motor Company v. Mont. Eighth Jud. Dist. Ct.,* 141 S.Ct. 1017, 1024 (2021).

[23] *International Shoe Co.,* 326 U.S. at 320.

[24] *See Burger King Corp. v. Rudzewicz,* 471 U.S. 462, 472-73 (1985); *Plixer*, 905 F.3d at 7.

[25] *Ford Motor Company,* 141 S.Ct. at 1024 (explaining that "our most common formulation of the rule demands that the suit 'arise out of or relate to the defendant's contacts with the forum.'" (citations omitted)).

[26] *Id.* at 1024 (citing *Hanson v. Denckla*, 357 U.S. 235, 253 (1958)).

[27] *Id.*; *A Corp. v. All American Plumbing, Inc.*, 812 F.3d 54 at 59 (1st Cir. 2016); *Plixer International, Inc.,* 905 F.3d at 7.

[28] *Goodyear Dunlop Tires Operations, S.A.,* 564 U.S. at 919 (2011) (internal quotation marks and brackets omitted); *Bristol-Myers Squibb Co. v. Super. Ct. of Cal.*, 137 S.Ct. 1773, 1780 (2017).

[29] *Ford Motor Company,* 141 S.Ct. at 1024 (2021) (citing *Hanson,* 357 U.S. at 253); *World-Wide Volkswagen Corp. v. Woodson*, 444 U.S. 286 (1980); *Carreras v. PMG Collins, LLC*, 660 F.3d 549, 555 ("Purposeful availment represents a rough quid pro quo: when a defendant deliberately targets its behavior toward the society or economy of a particular forum, the forum should have the power to subject the defendant to judgment regarding that behavior.").

[30] *Keeton v. Hustler Magazine, Inc.,* 465 U.S. 770, 774 (holding that the "general course of conduct in circulating magazines throughout the state was purposefully directed at New Hampshire.").

[31] *World-Wide Volkswagen Corp.,* 444 U.S. at 299; *Helicopteros Nacionales de Colombia, S.A.,* 466 U.S. at 41 (explaining that the courts aim to avoid exercising jurisdiction solely as a result of random, fortuitous, or attenuated contacts, or of the "unilateral activity of another party or a third person.); *Keeton* 465 U.S. at 774 (contrasting the defendants purposeful direction of business to the state with a "random, isolated, or fortuitous" act.).

In a series of decisions, the Supreme Court held that the exercise of specific personal jurisdiction was improper over (1) an out-of-state car manufacturer whose only tie to the forum resulted from the customer's decision to drive there,[32] (2) a divorced husband sued for child-support payments, whose only affiliation with the forum was his former spouse's decision to live there,[33] and (3) a trustee whose only connection with the forum resulted from the settlor's decision to exercise here power of appointment there.[34] Conversely, the Supreme Court held that a car manufacturer "purposefully availed" itself of a forum where it advertised its vehicles in the forum via multiple mediums, allowed the sale of its cars throughout the forum, and fostered ongoing connections with its cars' owners who lived in the forum.[35]

In 2018, the U.S. Court of Appeals for the First Circuit affirmed a federal district court's decision finding a German company, with no physical ties to the U.S., but that made its website globally available to businesses over the world had minimum contacts with the U.S. for the court to exercise personal jurisdiction over the company.[36] The German company did not have an office, phone number, or agent for service of process in the U.S., it did not advertise in the U.S., it accepted payment only in euros, its contracts provided that only German law governs disputes, which would be adjudicated in German courts, and its employees did not travel to the U.S. for business.[37] However, the German company's website was published in English, it did not attempt to limit access to its website to block U.S. users, nor did it "take the low-tech step of posting a disclaimer that its service is not intended for U.S. users".[38] and over the previous three years 156 of its customers were based in the U.S., with revenues just under $200,000 in June 2017.[39] Considering these factors, the First Circuit, noting that it was a close call, determined the German company should have "reasonably anticipated the exercise of specific personal jurisdiction based on its U.S. contacts.[40]

Finally, whether the exercise of jurisdiction is reasonable is only addressed once the court has decided that (1) the harm or controversy occurred in the U.S., and (2) the company purposefully availed itself of the U.S.[41] Notably, the reasonableness inquiry is often only discussed if the company's contacts with the U.S. are less than what would normally be required to satisfy the "purposeful availment" condition.[42] When looking at whether jurisdiction is reasonable, the courts look to whether exercising jurisdiction over a company would make litigation so difficult and inconvenient that the company is at a severe disadvantage in comparison to his opponent.[43] Because of the decreasing cost and increasing convenience of international travel, as well as new applications of

---

[32] *World-Wide Volkswagen Corp.,* 444 U.S. 286.

[33] *Kulko v. Cal. Super. Ct.,* 436 U.S. 84 (1978).

[34] *Hanson,* 357 U.S. 235.

[35] *Ford Motor Company*, 131 S.Ct. at 1028.

[36] *Plixer*, 905 F.3d at 12 (1st Cir. 2018).

[37] Id. at 4.

[38] Id. at 9.

[39] Id. at 4-5.

[40] Id. at 10.

[41] *Burger King Corp*., 471 U.S. at 476.

[42] *Id*.; *A Corp.* 812 F.3d at 59 (stating that "the weaker the plaintiff's showing on the first two prongs (relatedness and purposeful availment), the less a defendant need show in terms of unreasonableness to defeat jurisdiction").

[43] *Burger King Corp*., 471 U.S. at 476 (citing *Bremen v. Zapata Off-Shore Co.*, 407 U.S. 1, 18 (1972).

technology in litigation, courts are less likely to find that the inconvenience imposed on an EU Entity to try a case in the U.S. is enough to cause this inquiry to fail.[44]

For purposes of how courts may apply a specific personal jurisdiction analysis to the CLOUD Act, the Supreme Court has not definitively answered how online activities translate into "contacts" for purposes of the minimum contacts analysis. However, the Supreme Court has "reiterate[d] that the 'minimum contacts' inquiry principally protects the liberty of the nonresident defendant, not the interests of the plaintiff."[45]

With this in mind, and understanding that there is no bright line rule, the following can be used as a general guideline when determining whether an EU Entity who offers services or products to U.S. consumers is subject to the CLOUD Act:

1. If the EU Entity actively targets U.S. consumers (for example, by providing a separate U.S. website or engaging in targeted advertising in the U.S.), the EU Entity will likely be subject to the CLOUD Act.[46]
2. If the EU Entity passively offers its products or services to U.S. consumers (for example, by hosting a website that is generally available globally, but that in no way actively targets U.S. consumers) the EU Entity may be subject to the CLOUD Act depending on details such as revenue generated from the U.S. and the company's knowledge of its consumer base in the U.S.[47]
3. If the EU Entity intentionally tries to avoid targeting U.S. consumers (for example, by geofencing its website so that it is not accessible in the U.S.), but incidentally has contacts with U.S. consumers, the CLOUD Act will likely not apply to the EU Entity.[48]
4. If a middleman or third party vendor uses an EU Entity's products or services in the US, but the EU Entity does not itself target U.S. consumers, the CLOUD Act may not apply to the EU Entity.[49]

Question 3: Please list other relevant U.S. laws that could impact an EU Entity.

---

[44] *Id.* (explaining that modern travel "creates no especially ponderous burden for business travelers." The court also notes that many of the case's logistical challenges "can be resolved through the use of affidavits and video devices."); *Pritzker v. Yari*, 42 F.3d 53, 64 (1st Cir. 1994); *Hannon v. Beard*, 524 F.3d 275, 285 (1st Cir. 2008) (A defendant hoping to show that travel burdens should make the difference must show that those burdens are "special or unusual.").

[45] *Ford Motor Company,* 141 S.Ct. at n. 4; *Walden v. Fiore*, 571 U.S. 277, 290, n. 9 (in response to arguments that its decisions could "bring about unfairness in cases where intentional torts are committed via the Internet or other electronic means").

[46] *Burger King Corp.,* 471 U.S. at 475-76 (Explaining that the purposeful availment test is satisfied where the defendant deliberately engaged in significant activities in the forum.).

[47] *Kuan Chen v. U.S. Sports Academy, Inc.,* 956 F.3d 45 at 59-60 (1st Cir. 2020) (explaining that "specific targeting of a forum" is not the only means of showing that the purposeful availment test has been met. Other factors such as a regular course of sales or substantial revenue can also be used to show purposeful availment.)

[48] *Plixer,* 905 F.3d at 8 (explaining that the defendant could have taken steps to limit access to its website, such as designing the site to not interact with U.S. users or by posting a disclaimer that its service is not intended for U.S. users.).

[49] *Walden,* 571 U.S. at 284 (Stating that the relationship with the forum must arise out of the contacts that the defendant himself creates with the forum.); *Helicopteros Nacionales de Colombia, S.A.,* 466 U.S. at 417 ("[The] unilateral activity of another party or a third person is not an appropriate consideration when determining whether a defendant has sufficient contacts with a forum State to justify an assertion of jurisdiction").

Response: There are other U.S. laws that permit the U.S. government or U.S. courts to seek to access data stored by an EU Entity in the EU.[50] However, prior to the EU Entity being required to produce such data, the EU Entity would have the opportunity to file a motion to quash or modify an order on jurisdictional grounds, and to the extent the order seeks the content of electronic communications, cloud-stored documents, and non-content data relating to electronic communications, a court would apply the Cloud Act analysis described above in the responses to Questions 1 and 2.

As previously noted, the CLOUD Act amends two titles of ECPA – Title I (the Wiretap Act) and Title II (the SCA).[51] Pursuant to ECPA, law enforcement may access domestic and foreign subscriber data, including the content of the communications, of "wire or electronic communication service providers."[52] The term "electronic communications service providers" is defined to include "any service which provides to users thereof the ability to send or receive wire or electronic communications."[53]

Wiretap Act. The Wiretap Act prohibits the intentional actual or attempted interception, use, disclosure, or procurement of wire, oral, or electronic communications.[54] The Wiretap Act then creates a number of exceptions to this prohibition, including one in which the government to intercept communications or conduct electronic surveillance where it can show probable cause that intercepting communications will reveal evidence of a certain type of crime.[55] If the government can establish such probable cause, the court can issue a warrant authorizing the government to intercept communications for up to 30 days.[56] However, information collected through this process remains subject to limits on its use and disclosure.[57]

The CLOUD Act amends several provisions of the Wiretap Act to allow the U.S. government to enter into executive agreements with foreign governments which allow CSPs to comply with lawful foreign orders without regard to conflict-of-law issues.[58] The Wiretap amendment does not expand the U.S. government's power, it only creates a system whereby the U.S. government can cooperate with a foreign government in assuring that both governments can obtain necessary information without regard to conflict-of-law issues. [59]

---

[50] Pursuant to the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3414, certain U.S. law enforcement agencies may seek records from financial institutions. In addition, approximately 335 U.S. federal agencies have the ability to issue administrative subpoenas or civil investigatory demands compelling the production of documents or information from organizations, and U.S. courts, including the Foreign Intelligence Surveillance Court (FISC), have the ability to issue search warrants, subpoenas, and grand jury subpoenas on EU Entities which personal jurisdiction exists. In relation to FISA 702, see Expert Opinion on Current State of U.S. Surveillance Law and Authorities from Prof. Stephen I. Vladeck, University of Texas School of Law, 15 November 2021 at Vladek_Rechtsgutachten_DSK_en.pdf.

[51] While the ECPA also includes Title III, which addresses pen register and trap and trace devices, Title III was not amended by, and is not relevant to the CLOUD Act. 18 U.S.C. Chap. 206. Note that under Title III of ECPA, no actual communications are intercepted by a pen register or trap and trace.

[52] 18 U.S.C. § 2709(a) (2015).

[53] 18 U.S.C. § 2711(1) (2019) (incorporating definition found in 18 U.S.C. § 2510); 18 U.S.C. § 2510).

[54] 18 U.S.C. § 2511 (2018).

[55] 18 U.S.C. § 2516 (2018); 18 U.S.C. § 2517 (2002).

[56] 18 U.S.C. §2518 (1998).

[57] 18 U.S.C. § 2518(4-5) (1998).

[58] CLOUD Act § 103(a)(2) *et seq*.; 18 U.S.C § 2523 (2018).

[59] *Id.*

Stored Communications Act. The SCA governs the disclosure of user data, content, and non-content to law enforcement.[60] Section 2703 outlines the requirements for the disclosure of user information using search warrants, subpoenas, or court orders. While the SCA initially allowed law enforcement to obtain user content via a subpoena if the data had been stored for over 180 days, typically law enforcement is required to obtain a warrant to compel user content.[61]

The CLOUD Act directly amends the Stored Communications Act by adding Section 2713:

> A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[62]

The additional language does two things: (1) it defines CSPs to include "remote computing services" (the provision to the public of computer storage or processing services by means of an electronic communications system)[63] as well as "electronic communication services" (any service which provides users the ability to send or receive wire or electronic communications)[64], and (2) it clarifies that CSPs must comply with orders under the SCA regardless of whether such communication, record, or other information is located within or outside of the United States.[65] The DOJ has taken the position that the SCA Amendment does not expand the U.S. government's ability to obtain relevant information, it only clarifies the obligations under the SCA of providers subject to U.S. jurisdiction.[66]

Question 4: Please indicate whether the U.S. can obtain data from an EU Entity over whom it does not have jurisdiction by ordering a U.S. national who has access to data abroad to hand over data under the CLOUD Act or otherwise.

Response: In theory the answer is NO, in practice it is most likely YES. The CLOUD Act's amendment to the SCA states that CSPs must disclose data regardless of where the CSP stores the data.[67] Under the SCA, an order may only be made "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal

---

[60] Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Content is generally considered to include information, such as e-mail messages, while non-content information includes transactional or subscriber information. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA) 5 (2015), available at https://fas.org/sgp/crs/misc/R44036.pdf.

[61] A 2703(d) order is a combination of a warrant and a subpoena that allows law enforcement to obtain transactional information, such as user sign-in logs, but not email content.

[62] 18 U.S.C. § 2713 (2018).

[63] 18 U.S.C. § 2711(2) (2016).

[64] 18 U.S.C. § 2510(15) (2002).

[65] 18 U.S.C. § 2713 (2018); CLOUD Act § 103(a)(1) (2018).

[66] CLOUD Act Whitepaper 7.

[67] 18 U.S.C. § 2713.

Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice)."[68] Warrant procedures require that warrants only be issued over a person or entity that is subject to that court's jurisdiction. Thus, a lawful SCA order may not be issued for data belonging to an EU entity over which the U.S. government does not have jurisdiction by ordering a U.S. national who has access to such data abroad to access and produce such data. However, there are other means by which the U.S. government may attempt, as a practical matter, to obtain data located in the EU, from an individual who has access to data abroad or who is located abroad.

There are generally four ways the U.S. government may obtain information from a person or entity: voluntary consent, a warrant,[69] a subpoena,[70] and a civil investigative demand ("CID")[71]. Warrants, subpoenas, and CIDs are all subject to specific processes established by statute, and all are subject to questions of jurisdiction. Consent, on the other hand, is not a legal process and is therefore not subject to questions of jurisdiction. Generally, the U.S. government is free to ask people to voluntarily provide information, regardless of whether the U.S. government has jurisdiction over the person or related entity. Although there is a public perception that most people will refuse to consent to intrusive electronic searches, a recent study has called that widespread assumption into question. In reality, it appears that, if pressed, over ninety percent of people will consent to intrusive electronic search requests.[72] As a result, any reliance on protections provided by the formal legal requirements associated with warrants, subpoenas, and CIDS, may provide a false sense of security as the majority of people will voluntarily provide information to the government if asked to do so.

With respect to the U.S. government's ability to subject U.S. nationals to an involuntary access demand, a useful example can be made of the subpoena process. Subpoenas are perhaps the most common compulsory process the U.S. government uses to obtain information. In most cases, a subpoena commands a person to provide certain information within the person's possession, custody, or control.[73] Whether someone has possession, custody, or control of information is a fact-intensive inquiry. For example, if a U.S. national had information from or about an EU entity saved locally on his or her computer, that information would likely be considered to be in the national's "possession." If the U.S. national merely had the ability to remotely access information stored outside of the U.S., this is less likely to be considered to be within the U.S. national's possession but, depending on the circumstances, the government may argue that the information is in the U.S. national's custody or control.

The courts of the United States may order the issuance of a subpoena to a national or resident of the United States located in a foreign country to appear or to produce evidence.[74] The subpoena may direct the witness to appear in the United States or

---

[68] 18 U.S.C. § 2703(a).
[69] *See e.g.,* Fed Rules Crim Proc R 41(e)(2)(B).
[70] *See e.g.,* Fed Rules Crim Proc R 17.
[71] *See e.g.,* 31 U.S. § 3733 (regarding civil investigative demands for information relevant to a false claims law investigation).
[72] Sommers, Roseanna and Bohns, Vanessa K., The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance (April 10, 2019). Yale Law Journal, Vol. 128, No. 7, 2019, U of Michigan Law & Econ Research Paper No. 19-016, Available at SSRN: https://ssrn.com/abstract=3369844
[73] Fed. R. Civ. P. 45.
[74] 28 U.S.C. § 1783.

abroad (e.g., at an American Embassy or consulate). If the subpoenaed person fails to appear or otherwise comply with the subpoena, the court can order contempt sanctions which include seizing the person's property within the United States, and can the individual no more than $100,000.[75]

Although it is possible to challenge a subpoena in court, the government's ability to subpoena information has few restrictions — especially outside of the criminal context.[76] Of course, despite the government's legal limitations, challenging a subpoena requires the subpoenaed individual to object. A U.S. national is unlikely to object to a subpoena, especially in a situation where the U.S. national is not permitted to disclose the existence of the subpoena to his or her employer (in which case the employer may be able to object to the subpoena on the employee's behalf).[77] Practically speaking, the U.S. national would need to (1) understand that he or she is not required to comply with subpoena, (2) independently retain legal counsel, and (3) object to the demand. In the event the U.S. national did not object to the subpoena, or failed in his or her objection, the U.S. national may not distinguish between information saved locally and information available remotely (i.e., understand the scope of the data he or she is legally required to provide). As a result, there is a danger that an employee who is served with a subpoena may simply retrieve any amount of information from servers in the EU and turn it over in response to a government demand without ever notifying the EU employer.

Question 5: What happens if a foreign entity with no presence in the U.S., but who has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, ignores a CLOUD Act order?

Response: Assuming the foreign entity is subject to U.S. jurisdiction, the failure to respond to a Cloud Act warrant can result in monetary sanctions and possibly imprisonment. When a party ignores a Cloud Act warrant, the court will typically hold a hearing where the foreign entity has the opportunity to explain the reason for non-compliance. U.S. courts typically have broad discretion to determine an appropriate punishment given the circumstances presented. In one matter, involving the enforcement of a grand jury subpoena in relation to a foreign entity (but not involving a Cloud Act order), the appeals court fined the foreign entity $50,000 per day for each day that the foreign entity refused to comply with a grand jury subpoena.[78] Although it is questionable how such a fine would actually be collected from a foreign entity without a U.S. present. In some cases, the U.S. may be able to convince government authorities in the member state where the foreign entity is based to assist with such enforcement. And of course, should the foreign entity eventually have a presence in the U.S., the U.S. government may be able to then pursue enforcement of such fine, or seize the foreign entity's property in the U.S.

---

[75] 28 U.S.C. § 1784.
[76] *See, e.g.*, *McLane Co., Inc. v. E.E.O.C.*, 137 S. Ct. 1159, 1169 (2017), as revised (Apr. 3, 2017).
[77] *Cf. Matter of Subpoena 2018R00776*, 947 F.3d 148, 158–59 (3d Cir. 2020) (upholding constitutionality of nondisclosure order accompanying a warrant).
[78] *See In Re Grand Jury Subpoena*, Case No. 18-3071 (D.C. Cir. Dec. 18, 2018), *cert. denied* (U.S. Sup. Ct. Jan. 8, 2019) (https://www.supremecourt.gov/orders/courtorders/010819zr1_m6hn.pdf). See *In Re Grand Jury Subpoena*, Case No. 18-3071, (D.C. Cir. Jan. 8, 2019), expanded decision at https://www.cadc.uscourts.gov/internet/opinions.nsf/543298E5B1BEA87C8525837C0074E9A9/$file/18-3071-PUBLIC.pdf

Question 6: With respect to an EU Entity who has no presence in the U.S., but who has sufficient contacts with the U.S. such that it is reasonable for the U.S. to assert jurisdiction over the EU Entity, please indicate whether all data that is in this EU Entity's custody, control, or possession fall within the purview of the CLOUD Act, or only that data which relates to a U.S. citizen.

Response: When the U.S. government is relying on the CLOUD Act's amendment to the SCA, an EU Entity can move to quash or modify a warrant, subpoena or court order where the EU Entity believes:

(i) that the warrant conflicts with the law of a foreign country that has not entered into an international agreement authorized by the Cloud Act (common law comity challenge); or
(ii) that the customer or subscriber is not a United States person and does not reside in the United States; and that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.[79]

The U.S. Department of Justice, in an oral argument before the U.S. Supreme Court, recognized the availability of common law comity challenges, noting that when U.S. legal process conflicts with a foreign law "courts conduct a comity analysis."[80] In fact, the CLOUD Act specifically provides that, "[n]othing in this section, or an amendment made by this section, shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process."[81] Under the common-law comity analysis, in considering whether to modify or quash the warrant, courts may look to factors such as:

- The importance of the information requested.
- The degree of specificity of the request.
- Whether the information originated in the U.S.
- The availability of alternative means to obtain the information.
- The U.S. and foreign interests at stake.[82]

Courts may modify or quash a warrant when considered together, these factors weigh in favor of the challenge. And in contrast to the statutory framework under the CLOUD Act (addressed below), a common-law challenge is available even where the customer or subscriber is a U.S. person or resides in the U.S.

Under the statutory framework, a court may modify or quash the order only if it finds:

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

[79] 18 U.S.C. § 2703(h)(2)(A).
[80] Transcript of Oral Argument at 27, United States v. Microsoft Corp., No. 17-2 (2018), available at https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/17-2_j4ek.pdf.
[81] 18 U.S.C. § 2713(c).
[82] *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 544 n.28 (1987); *see* Restatement (Third) of the Foreign Relations Law of the United States § 442 (1987).

> (iii) the customer or subscriber is not a United States person and does not reside in the United States.[83]

The EU Entity will bear the burden of demonstrating that foreign law does, in fact, prohibit disclosure of the information sought.[84]

In determining whether the interests of justice should require an EU Entity to produce information, the U.S. courts consider the following factors:

> (A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;
> (B) the interests of the qualifying foreign government in preventing any prohibited disclosure;
> (C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;
> (D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to [18 U.S.C.] section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;
> (E) the nature and extent of the provider's ties to and presence in the United States;
> (F) the importance to the investigation of the information required to be disclosed;
> (G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and
> (H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.[85]

While an EU Entity can seek to modify the order to have it limited to only that information relating to U.S. residents, this is just one factor that U.S. courts consider in determining whether to modify such order. Thus, the success of an EU Entity in having the order limited to apply only to the data of U.S. residents' data will depend on the specific circumstances relevant in relation to such request, and courts could find the other factors outweigh limiting the order to just U.S. residents, which would result in EU residents data from also being produced.

If the U.S. government is relying on a bi-lateral agreement executed pursuant to the CLOUD Act's amendment to the Wiretap Act, the scope and reach of a CLOUD Act order will depend on how the foreign government negotiated the agreement. As mentioned above there is no such agreement in place with any EU member state. As a threshold matter, foreign governments are prohibited from using CLOUD Act orders to intentionally

---

[83] 18 U.S.C. § 2703(h)(2)(B).
[84] *United States v. Vetco Inc*., 691 F.2d 1281, 1289 (9th Cir. 1981).
[85] 18 U.S.C. § 2703(h)(3).

target a U.S. person located within or outside the U.S.[86] While the CLOUD Act does not include specific language stating the same for foreign nationals, the foreign government is free to seek similar restrictions that would prevent the United States from using orders to target data of the foreign country's residents.[87] To the extent the foreign government limits the scope of U.S. government orders made pursuant the Wiretap Act to exclude information about foreign nationals, then only that data which relates to a U.S. citizen will fall within the purview of the CLOUD Act.

Closing remarks

While it is possible to ringfence against the CLOUD Act as described above we note that:

i. proper encryption (like Microsoft's DKE[88]) will prevent access to most data;
ii. a risk-based approach as taken in the DPIA on Teams[89] could well lead to the conclusion that the risks are low; and
iii. although not all details are known yet, Microsoft's new EU Data Boundary, combined with changes to its business model, as announced by Microsoft's President Brad Smith in Brussels recently[90], seem to prevent any data going from the EU to the US and might also contain a ringfence against the CLOUD Act. The French initiative *Bleu*, from Capgemini, Orange (with Microsoft) seems to be structured that way, but not all details are public yet. Google is reportedly working on similar initiatives.
iv. the CLOUD Act may also reach data via sub-contractors/providers of hardware and software from/to cloud providers. As an example, if Microsoft uses Cisco routers and Cisco has access to data from EU customers/data subjects via these routers, this will also need to be adressed.

[86] 18 U.S.C. § 2523(b)(4)(A-B).

[87] CLOUD Act Whitepaper FAQ 6 at pg. 12.

[88] Microsoft Double Key Encryption (slmmicrosoftrijk.nl)

[89] link

[90] Microsoft responds to European Cloud Provider feedback with new programs and principles - EU Policy Blog