Hogan Lovells

Demystifying the U.S. CLOUD Act:

Assessing the law's compatibility with international norms and the GDPR

Hogan Lovells | January 2019

Hogan Lovells

Demystifying the U.S. CLOUD Act:

Assessing the law's compatibility with international norms and the GDPR

Winston Maxwell

Partner, Paris
+ 33 1 53 67 48 47
winston.maxwell@hoganlovells.com

Mark W. Brennan

Partner, Washington, D.C.
+ 1 202 637 6409
mark.brennan@hoganlovells.com

Arpan A. Sura

Senior Associate, Washington, D.C.
+ 1 202 637 4655
arpan.sura@hoganlovells.com

Executive summary

This paper discusses the impact of a new U.S. law – the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) – on non-U.S. businesses and individuals who use cloud storage solutions. The CLOUD Act amends the Stored Communications Act (SCA), which restricts the disclosure of stored electronic data to third parties, including the U.S. government. This paper specifically focuses on Part 1 of the CLOUD Act, which clarifies that U.S. law enforcement agencies may, under certain circumstances, lawfully demand data stored in foreign countries from entities subject to U.S. jurisdiction.[1] Some commentators have worried that Part 1 of the CLOUD Act will give the U.S. government new powers to surveil the data of any non-U.S. citizen or business that uses a cloud services provider with operations in the United States.

This paper concludes, however, that such worries are overstated in at least two respects. Part 1 of the CLOUD Act does not represent a radical change; rather, it largely clarifies that a settled body of pre-existing case law applies to the SCA. Nor do we expect the CLOUD Act to enhance the capacity of U.S. law enforcement to collect non-U.S. citizens' data stored outside the United States; there are numerous legal and practical safeguards in place that would prevent such an outcome. This paper makes the following key points regarding Part 1 of the CLOUD Act.

- ***The CLOUD Act is a return to the status quo.*** The assumption that the CLOUD Act heralds a sea change in the SCA is inaccurate. Before the CLOUD Act, most courts had held that U.S. law enforcement agencies could reach data stored extraterritorially under the SCA, but only from a U.S. entity that had "possession, custody, or control" over the data. The notable exception, of course, was the 2nd Circuit's decision in *Microsoft v. United States* that prompted Congress to pass the CLOUD Act. The CLOUD Act effectively vacated *Microsoft* and restored the legal consensus that existed previously among American courts.
- ***The CLOUD Act retains meaningful limitations on U.S. law enforcement.*** The CLOUD Act does not expand access to foreign data by the U.S. government. In particular, there are several limitations on the U.S. law enforcement's ability to request the data of foreign users under the CLOUD Act. First and foremost, the entity to which a CLOUD Act request is issued must be an applicable service provider subject to U.S. jurisdiction. Second, that entity must have "possession, custody, or control" over the data. Third, the request must otherwise comply with the statutory strictures of the SCA and, where applicable, the Fourth Amendment to the U.S. Constitution. Finally, any warrant or subpoena would be governed by the CLOUD Act's statutory comity framework, as well as the common-law principles of international comity that the U.S. Supreme Court articulated in its Société Nationale Industrielle Aérospatiale decision.

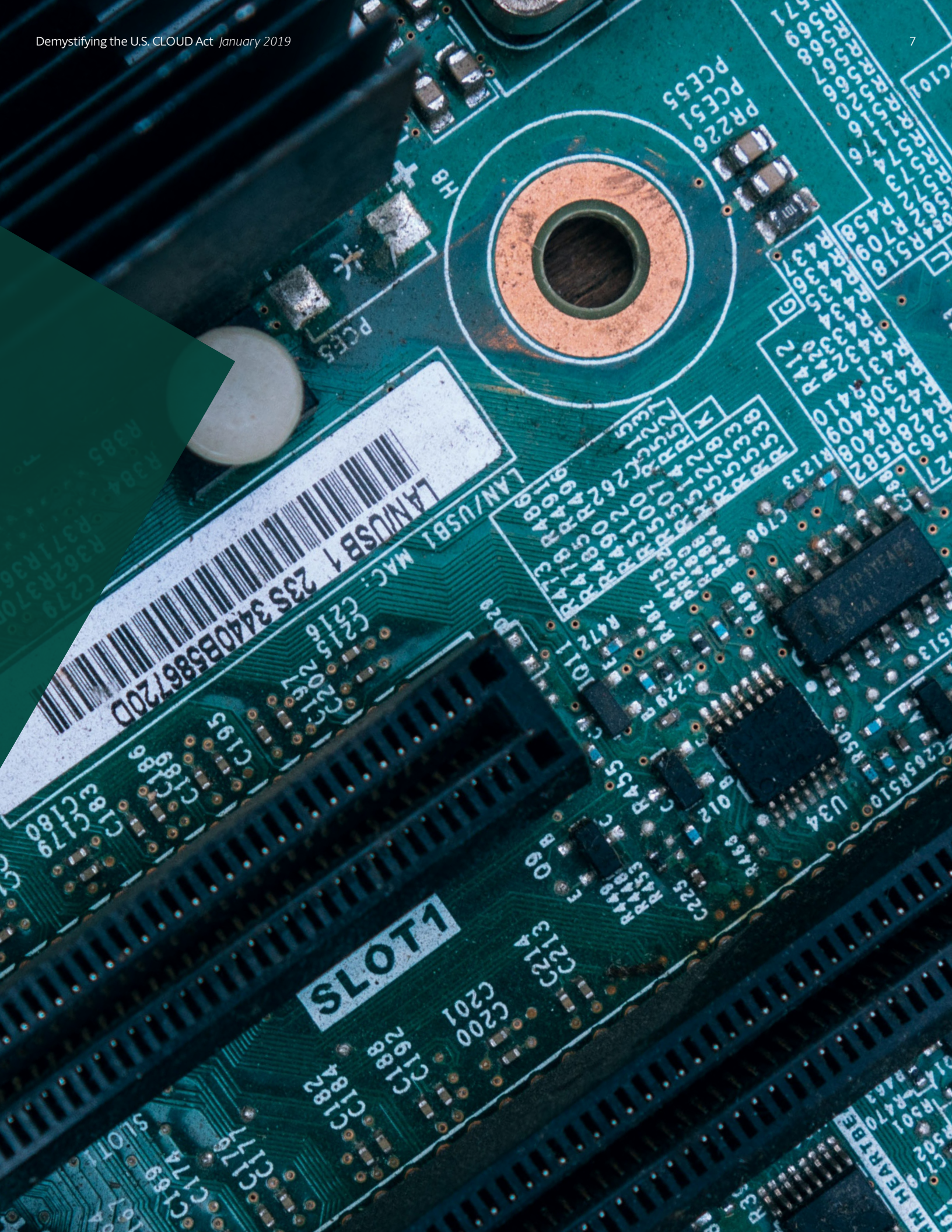
- ***The CLOUD Act is consistent with the European Union's approaches to criminal investigations.*** The European Union has proposed an e-evidence regulation that would allow production orders in criminal investigations without regard to the physical location of the data servers. Such a regulation would be in line with Part 1 of the CLOUD Act. Meanwhile, the power of U.S. judges under the SCA to order production of evidence under a provider's "possession, custody, or control" appears to be consistent with the Council of Europe's Cybercrime Convention. Simply put, there does not appear to be a major difference in how the European Union and the United States are approaching the fundamental issue of cross-border data requests from law enforcement.
- ***The CLOUD Act does not violate international law or the GDPR.*** Some have worried that the CLOUD Act creates an inconsistent set of legal obligations on non-U.S. citizens or businesses, including EU businesses that are subject to the General Data Protection Regulation (GDPR). Frictions between the power of U.S. judges to compel the production of evidence and European data protection law existed already under the 1995 Data Protection Directive, and neither the CLOUD Act nor the GDPR changes the fundamental legal considerations for cross-border data transfers to U.S. law enforcement authorities. The GDPR states that transfer of data to U.S. authorities should be done under international agreement such as Mutual Legal Assistance Treaties (MLATs), but that is not the exclusive legal basis for transfer as the European Commission explained in its amicus brief to the U.S. Supreme Court.

In sum, the SCA, which has been in operation since 1986, remains intact following the passage of Part 1 of the CLOUD Act. Part 1 of the CLOUD Act clarified an ambiguity in the statutory language of the SCA, siding with the interpretation held by a majority of U.S. federal courts that the physical location of data is not relevant under the SCA. This interpretation appears to be consistent with international trends, including the Council of Europe Cybercrime Convention and the proposed EU e-evidence regulation.

---

1 This paper focuses only on Part 1 of the CLOUD Act. Part 2 of the CLOUD Act, which we do not examine, permits the U.S. government to enter into executive agreements (EAs) with other countries that meet baseline privacy, due process, and human rights standards. The EAs are intended to facilitate streamlined data access for foreign law enforcement authorities in the investigation of serious crimes, provided that they meet baseline privacy, due process, and human rights standards under the CLOUD Act. The CLOUD Act contains certain additional provisions besides Parts 1 and 2. Such provisions are also outside the scope of this paper.

Contents


LAN/USB1 MAC:
SLOT1

I. Introduction and background

On 23 March 2018, President Trump signed into law the Clarifying Overseas Use of Data Act (CLOUD Act). The CLOUD Act amends a U.S. privacy law known as the Stored Communications Act (SCA), which restricts the disclosure of stored electronic data to third parties, including the U.S. government. The CLOUD Act contains two important provisions. First, it requires that certain internet-based service providers subject to U.S. jurisdiction "disclose the contents of ... an 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" (Part 1 of the CLOUD Act). Second, the CLOUD Act allows foreign governments to enter into new bilateral executive agreements (EAs) with the United States. These EAs would permit streamlined foreign law enforcement requests directly to U.S. service providers and would complement the procedures in existing Mutual Legal Assistance Treaties (MLATs) and common-law principles of international comity (Part 2 of the CLOUD Act). No EAs are yet in effect. This paper examines the first part of the CLOUD Act, the part that states that the location of data is not relevant for purposes of production orders issued under the SCA.

By clarifying U.S. law enforcement's ability to reach data stored abroad, the CLOUD Act sparked considerable discussion in the international community. Some commentators in the European Union, for example, criticized the CLOUD Act as a threat to global civil liberties. They warned that the CLOUD Act would expand U.S. government access to the data of EU citizens and businesses. Businesses in the European Union, meanwhile, worried that the CLOUD Act would threaten the privacy and security of their data hosted or stored on cross-border cloud networks.

A few common themes have emerged from these disparate criticisms: the CLOUD Act is a novel expansion of U.S. power; it will jeopardize territorial sovereignty; and it will undermine the privacy interests created by jurisdiction-specific laws, such as the General Data Protection Regulation (GDPR) in Europe.

This paper evaluates the merit of these claims and finds them overstated and in some cases inaccurate. Assessing the impact of the CLOUD Act on global cloud solutions requires a proper understanding of: (i) the background statute – the SCA – that the CLOUD Act amended; and (ii) the 2nd Circuit's decision in *Microsoft v. United States* that caused the U.S. Congress to pass the CLOUD Act in response. Read against this backdrop, the CLOUD Act

---

[2] Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, §§ 101-106, 132 Stat. 348, 1213-25 (2018).

[3] *Id.* § 103(a)(1), 132 Stat. 1214.

[4] For example, the European Parliament issued a nonbinding resolution on 5 July 2018 that calls on the European Commission to suspend the EU-U.S. Privacy Shield unless U.S. authorities can "fully comply" with the framework by 1 September 2018. In particular, the resolution "expresses strong concerns" about the CLOUD Act, which is viewed as having "serious implications for the European Union, as it is far-reaching and creates a potential conflict with the EU data protection laws." Motion for a resolution, to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) (5 July 2018), found here.

largely reaffirmed the established legal view – namely, the court in the *Microsoft* decision misinterpreted the SCA by adopting a bright-line rule based on the data's physical location. The prevailing legal authority interpreting the SCA examines whether the recipient of a request has "possession, custody, or control" of the data, not whether the data is physically located outside the United States. The "possession, custody, or control" criteria are flexible, allowing judges to evaluate the specific facts surrounding each criminal investigation. These flexible criteria are part of international standards in the field of criminal investigations, appearing in Article 18 of the Council of Europe's Cybercrime Convention.

A proper understanding of the SCA also shows why the CLOUD Act does not undermine key privacy protections. The SCA allows U.S. law enforcement to obtain data under limited circumstances – for example, the SCA applies only to certain types of service providers subject to U.S. jurisdiction, and it requires probable cause before a judge can issue a warrant for certain stored content. The CLOUD Act has not changed these legal requirements for lawful access, which are also consistent with EU fundamental rights standards.

TThe rules of criminal procedure generally seek to avoid bright-line legal tests that would make it easy for suspected criminals to move evidence to convenient hiding places outside the country. That is one of the reasons why the physical location of data servers has become largely irrelevant under rules of criminal procedure, as courts and law enforcement authorities apply a more flexible and fact-specific standard like Article 18 of the Council of Europe's Cybercrime Convention. That flexibility is then counter-balanced by robust procedural and human rights protections to avoid judicial and prosecutorial overreaching.

This paper proceeds as follows. Section II describes the operation of the SCA and the CLOUD Act. The CLOUD Act preserves virtually all of the SCA's statutory privacy protections that have functioned for decades. Section III examines the outlier *Microsoft* case, which led Congress to intervene and clarify the meaning of the SCA. Section IV then explains the ways in which the CLOUD Act is consistent with international legal norms. In particular, the CLOUD Act is largely interoperable with the principles of international law, the GDPR, and the Council of Europe Cybercrime Convention No. 185.

II. Back to the future: The CLOUD Act restores the functioning of the SCA as it existed for decades

A. Overview of the SCA

The expressed concerns of some EU stakeholders appear to be grounded on the notion – however vague – that the CLOUD Act gives the U.S. government expansive new power over data stored all over the world, but that fear is inaccurate and misplaced. The CLOUD Act is not a departure from prior precedent. Its core provision overturns the 2nd Circuit's *Microsoft* decision and instead sides with the majority of prior court decisions that reject *Microsoft*'s reasoning. These courts had held that the physical location of the data does not matter under the SCA so much as the party who controlled it. "Control, not location" has been the prevailing rule, notwithstanding *Microsoft*, and the CLOUD Act simply confirms the rule.[5]

Before examining *Microsoft* in detail, some background about the SCA is necessary. The Stored Communications Act permits the government to compel an "electronic communications service" (ECS) or "remote computing service" (RCS) – including a cloud service – to disclose its customers' data to law enforcement under certain circumstances.[6] Although the statute's requirements are discussed in greater detail below, three broad limitations on the act's scope are worth noting at the outset.

First, courts have held that the SCA limits law enforcement to data that an ECS or RCS has in its "possession, custody, or control."[7] That is the same standard that applies to civil discovery – including international e-discovery – in the United States.[8] Under the "possession, custody, or control" test, the "location of the information sought … is irrelevant."[9] That is also the relevant test under the Council of Europe's Cybercrime Convention, as we discuss in Section IV.

Second, the SCA includes a number of additional statutory safeguards that meet or exceed the protections afforded under the U.S. Constitution. For example, it does not apply to an entity that is not an ECS or RCS. Moreover, the SCA provides that law enforcement may obtain the contents of communications stored for less than 180 days only if it satisfies the traditional requirements for a search warrant, governed by the Fourth Amendment to the U.S. Constitution and Federal Rule of Civil Procedure 41.

Third, notwithstanding the SCA's protections, some courts have held that law enforcement requests for the contents of communications are always "searches" within the meaning of the Fourth Amendment, no matter how long the communications have been stored.[10] That means the government must show "probable cause" to believe that the information sought will contain evidence of a crime.

---

[5] The concept of "control" under U.S. case law relating to criminal and civil procedure is unrelated to the concept of "controller" under the GDPR.

[6] *See Orin Kerr, A User's Guide to the Stored Communications Act, 72 Geo. Wash. L. Rev. 1208, 1212 (2004); 18 U.S.C. §§ 2702(a)(3), (b)(2), (c)(1).*

[7] *See, e.g., Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 453 (C.D. Cal. 2007)*

[8] *See Fed. R. Civ. P. 34(a)(1).*

[9] *United States v. Martin, No. CR-14-00678-PHX-DGC (D. Ariz. 21 July 2015) (order denying motion to suppress).*

[10] *See United States v. Warshak*, 631 F.3d 266, 282 (6th Cir. 2010).

B. ECS/RCS requirement

The SCA imposes another statutory restriction on U.S. law enforcement – the recipient of a lawful recipient warrant, subpoena, or other request must be an RCS or ECS. If the recipient is not an RCS or ECS, then the request is invalid under the SCA. Whether an entity qualifies as an RCS or ECS is context-specific, and an entity can be an RCS or ECS (or both) with respect to some data but not others.

The term "remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communication system."[11] To be an RCS, a company essentially must offer value-added data storage services to the public. The statute's legislative history explains that such services exist to provide sophisticated and convenient data processing services to subscribers and customers, such as hospitals and banks, from remote facilities.[12] There are two key limitations on whether an entity qualifies as an RCS.

First, a company does not become an RCS solely because it stores data incidental to its primary business. For example, a defendant that stored a client's employees' personal information was held not to be an RCS with respect to that data; storage was incidental to the defendant's main service of providing the employees with a way to purchase household goods through payroll deductions.[13] Similarly, an airline that compiled and stored passenger information and itineraries through its website was not an RCS because these functions were incidental to providing airline reservation service.[14] Likewise, an e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users."[15]

Second, a company does not provide an RCS to the extent it is not available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, an employer that provides email accounts to its employees is not an RCS with respect to those employees' data, because such email accounts are not available to the public.[16] As another example, Pandora's cloud music-streaming service was not deemed an RCS because there was no allegation that users could upload or store content.[17]

---

[11] 18 U.S.C. § 2711(2).

[12] *See S. Rep. No. 99–541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564.*

[13] *Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 WL 9391827, at *5 (S.D. Fla. 18 Oct. 2012).*

[14] *In re Jetblue Airways Corp. Privacy Litigation, 379 F.Supp.2d 299 (E.D.N.Y. 2005).*

[15] *United States v. Standefer, 2007 WL 2301760, at *5 (S.D. Cal. 8 Aug. 2007).*

[16] *See Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

[17] *Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 WL 1282980, at *9 (N.D. Cal. 26 Mar. 2013).*

An "electronic communications system" is "any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[18] An ECS generally provides user access to a central computer system through which to send electronic messages over telephone or other communications lines. While the typical ECS includes internet service providers, email providers, and bulletin boards, it is possible for an online business or retailer to become an ECS if it has a website that offers customers the ability to send messages or communications to third parties.[19] In other cases that do not involve messaging services, courts regularly conclude that ordinary businesses providing services through the internet are not an ECS.[20]

C. Jurisdictional requirements

Under the SCA and the Due Process Clause of the U.S. Constitution, a warrant or subpoena may be directed to an ECS or RCS only if that entity is subject to "personal jurisdiction" in the United States.[21] The concept of "personal jurisdiction" (which arises under the U.S. Constitution) is distinct from the concept of "territorial jurisdiction" (which is implicated, for example, under the CLOUD Act). At a high level, the question of "personal jurisdiction" asks whether a person or company has sufficient "contacts" with a forum to be subject to its authority. The questions of to what extent a non-U.S. citizen or business is subject to U.S. jurisdiction in any particular case are highly dependent upon the particular facts of each matter.

Independent of the CLOUD Act, then, a warrant or subpoena under the SCA cannot reach a company over which the court lacks "personal jurisdiction."[22] Therefore, a U.S. court may lack "personal jurisdiction" over a U.S. or foreign entity, even if that entity exercises "control" over the data stored overseas under the CLOUD Act.

---

[18] 18 U.S.C. § 2510(14).

[19] *Kaufman v. Nest Seekers, LLC, 2006 WL 2807177, at *6 (S.D.N.Y. 2006) ("An on-line business which provides its customers, as part of its commercial offerings, the means by which the customers may engage in private electronic communications with third-parties may constitute a facility through which electronic communication service is provided.").*

[20] *See Walsh Bishop Assocs., Inc. v. O'Brien*, 2012 WL 669069, at *4-5 (D. Minn. 28 Feb. 2012) (holding that because "[c]ourts interpret the [ECPA/SCA] to encompass internet service providers and telecommunications companies" an architectural firm was not a provider of "electronic communications service" and failed to state a claim under the Act against an employee who accessed information on the firm's computer system); *Keithly v. Intelius Inc.*, 764 F.Supp.2d 1257, 1271-72 (W.D. Wash. 2011), *on reconsideration* 2011 WL 2790471 (holding that a company that uses electronic communications services to conduct its business on the internet but does not provide the wire or electronic communications services utilized by its customers was not an internet service provider, a telecommunications company, or a public carrier of any kind, and is therefore was not an "electronic communications service" subject to the protections of the SCA).

[21] *See*, e.g., U.S. Const. amend. XIV.

[22] *See In Re Search Warrant No. 16-960-M-1 to Google*, No. 2:16-mj-00960-JS (E.D. Pa. 17 Aug. 2017) (memorandum affirming magistrate judge's order) ("In manner of operation, then, an SCA warrant is 'more closely analogous to the workings of subpoenas and court-ordered discovery,' forms of legal process generally understood to be capable of reaching records in the possession or control of a party of which the enforcing court has personal jurisdiction, regardless of where the records are located, without raising extraterritoriality concerns.") (internal citation omitted).

D. "Possession, custody, or control" requirement

The CLOUD Act clarifies that an RCS or ECS served with legal process under the SCA must turn over data that is within its "possession, custody, or control," regardless of where such data is stored:

> "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."[23]

The "possession, custody, or control" standard has been extensively litigated in other contexts, namely the Federal Rules of Civil Procedure. Rule 34 provides that records may be sought where they are in the "possession, custody, or control" of a party to the litigation. While the terms "possession" and "custody" are fairly straightforward (basically amounting to physical possession), the legal definition of "control" is far less clear. In the context of document requests served on corporations, U.S. courts have generally applied one of two competing tests to determine if records possessed by a nonparty corporate affiliate or independent third party can be considered to be within the party's "control."[25]

Most courts today apply a broad equitable standard known as the "practical ability" test. This is a multifactored analysis under which a court will generally order document production if it "find[s] that a company's ability to demand and have access to documents in the normal course of business gives rise to the presumption that such documents are in the litigating corporation's control."[26] Numerous courts have applied a multifactor test and held that a U.S. subsidiary can have control over documents stored by its foreign parent.[27] Some of these factors include: (1)

---

[23] 18 U.S.C. § 2713.

[24] *Fed R. Civ. P. 34(A)(1).*

[25] As noted above, the concept of "control" discussed in this section should not be confused with the concept of "controller" under the GDPR. The two concepts are different.

[26] *Jonathan D. Jordan, Out of "Control" Federal Subpoenas: When Does a Nonparty Subsidiary Have Control of Documents Possessed by a Foreign Parent?, 68 Baylor L. Rev. 189, 200-01 (2016).*

[27] *See, e.g., In re Subpoena Duces Tecum to Ingeteam, Inc.*, No. 11-MISC-36, 2011 WL 3608407, at *1 (E.D. Wis. 16 Aug. 2011) (using five factors to measure "whether a subsidiary has 'control' over documents held by its foreign parent corporation"); *In re Subpoena to Huawei Techs. Co.*, 720 F. Supp.2d 969, 976 (N.D. Ill. 2010) (using seven factors to measure "the closeness of the relationship between the parties"); Stella v. *LVMH Perfumes & Cosmetics USA, Inc.*, No. 07-CV6509, 2009 WL 780890, at *2 (N.D. Ill. 23 Mar. 2009) (using four factors to measure "[t]he degree of control, [which] is determined by the 'closeness of the relationship between the entities'"); *In re Ski Train Fire of Nov. 11, 2000 Kaprun Austria,* No. MDL 1428(SAS)THK, 2006 WL 1328259 (S.D.N.Y. 16 May 2006) (the parent could not shield documents behind a formalistic control analysis when the parent dominated the subsidiary's board of directors).

ccommonality of ownership; (2) exchange or intermingling of directors; (3) the exchange of documents in the ordinary course of business; (4) the nonparty's connection to the transaction at issue; (5) any benefit or involvement by the nonparty corporation in the matter; (6) a subsidiary's marketing and/or servicing of the parent company's products; and (7) the financial relationship between the companies. A minority of courts conduct a narrower inquiry relating to control known as the "legal right" test, which defines "control" under Rule 34 as "the legal right to obtain documents requested upon demand."[28] Under this stricter approach, the party's practical ability to obtain the documents is irrelevant absent legal entitlement.

The control test is necessarily flexible and fact-specific, which is understandable in the context of criminal investigations, where criminal defendants may attempt to keep incriminating evidence outside the reach of U.S. prosecutors.

Regardless of the standard used, the "possession, custody, or control" test continues to be a substantive limitation on document discovery requests. As one example, one court found that a parent corporation did not exercise the level of control over its subsidiary necessary to have "control" over its documents for Rule 34 purposes.[29] IIn that case, the court concluded that "while [the parent's] ownership of its subsidiaries is a factor favoring plaintiffs in their bid for the foreign subsidiaries' documents, the lack of any track record in which [the parent] has actually exerted control points in the opposite direction."[30] It did not, as the court pointed out, participate in its subsidiaries' decision-making or monitor their activities, and furthermore did little "to independently verify the financial information they provide as inputs to [the parent's] consolidated financial statements."[31]

As these cases make clear, the "possession, custody, or control" test constitutes a meaningful constraint on law enforcement requests for data held by a non-U.S. entity under the CLOUD Act.

E. No direct access to data

The SCA establishes a legal process that regulates the ability of U.S. law enforcement to order RCS and ECS providers to disclose evidence. The SCA requires U.S. government entities to meet certain standards of proof to obtain the customer information of an RCS or ECS. These standards will depend on the type of information sought. The SCA does not allow law enforcement to extract data directly from systems, and the CLOUD Act does not eliminate or modify these procedural safeguards.

To access contents of electronic communications – including emails – that have been in electronic storage for less than 180 days, the SCA requires the government to obtain a search warrant from a judge.[32] One court has recently articulated that standard as follows: "Probable cause to search a location

---

[28] *United States v. Int'l Union of Petroleum & Indus. Workers, AFL-CIO*, 870 F.2d 1450, 1452 (9th Cir. 1989).

[29] *Stream Sicav v. Wang, 2014 U.S. Dist. LEXIS 81098 (S.D.N.Y. 12 Jun. 2014).*

[30] *Id.* at *16.

[31] *Id.* at *15.

exists if, based on the totality of the circumstances, there is a 'fair probability' that evidence of a crime may be found there."[33] Thus, where there is no "fair probability" of evidence relating to a crime, the SCA does not permit U.S law enforcement to obtain the email. The probable cause standard is one of the highest under U.S. law with regard to law enforcement. It derives from the Fourth Amendment of the U.S. Constitution and governs, among other things, wiretaps and police searches of homes or cars.

The government may obtain non-content records (e.g., network logs) or emails that have been stored for longer than 180 days through a subpoena or a "court order" issued under the SCA,[34] both of which require a lower showing than probable cause. The requirements for subpoenas vary by jurisdiction and statute, but they generally require that the subpoena be designed to produce documents relevant to a lawful investigation. Similarly, an SCA court order can be issued only if the records sought "are relevant and material to an ongoing criminal investigation."[35] Here again, U.S. law enforcement must show some nexus to a crime.

Independent of the SCA and the CLOUD Act, some courts have held that the Fourth Amendment to the U.S. Constitution requires a warrant based on "probable cause" for law enforcement to obtain stored email. The leading authority, Warshak, held that a warrant is necessary to obtain emails under the SCA's procedures, and "to the extent that the SCA purports to permit the government to obtain such emails without warrant, the SCA is unconstitutional."[36] In the wake of Warshak, it has been the policy of the U.S. Department of Justice since 2013 to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process.[37] Moreover, the U.S. prosecutors' handbook prepared by the Department of Justice regulates how federal prosecutors should handle cross-border data requests. The handbook makes clear that prosecutors must advance with great care and get clearance from the Criminal Division's Office of International Affairs.[38]

As we discuss in Section IV, moreover, the "probable cause" threshold for SCA warrants protects individuals to a similar extent as EU laws on fundamental rights. In the context of their review and criticisms of the former Safe Harbor regime, the European Commission and European Court of Justice have never raised concerns regarding the U.S. regime for criminal investigations.

---

[32] 18 U.S.C. § 2703(a).

[33] *United States v. Perkins, 850 F. 3d 1109, 1119 (9th Cir. 2017).*

[34] 18 U.S.C. § 2703(b).

[35] *Id. § 2703(d).*

[36] *Warshak*, 631 F.3d at 288.

[37] H.R. Rep. No. 114-528, at 9 (2016).

[38] *See* Dep't of Justice, U.S. *Attorneys' Manual* §§ 9-13.500-510 (last updated 2018).

Neither the SCA nor the CLOUD Act displace other methods of seeking information from service providers; rather, they add extra restrictions before an ECS or RCS can disclose customer information. If a law enforcement request or an administrative agency request is for information stored on a server subject to the SCA, the request will be subject to the SCA.

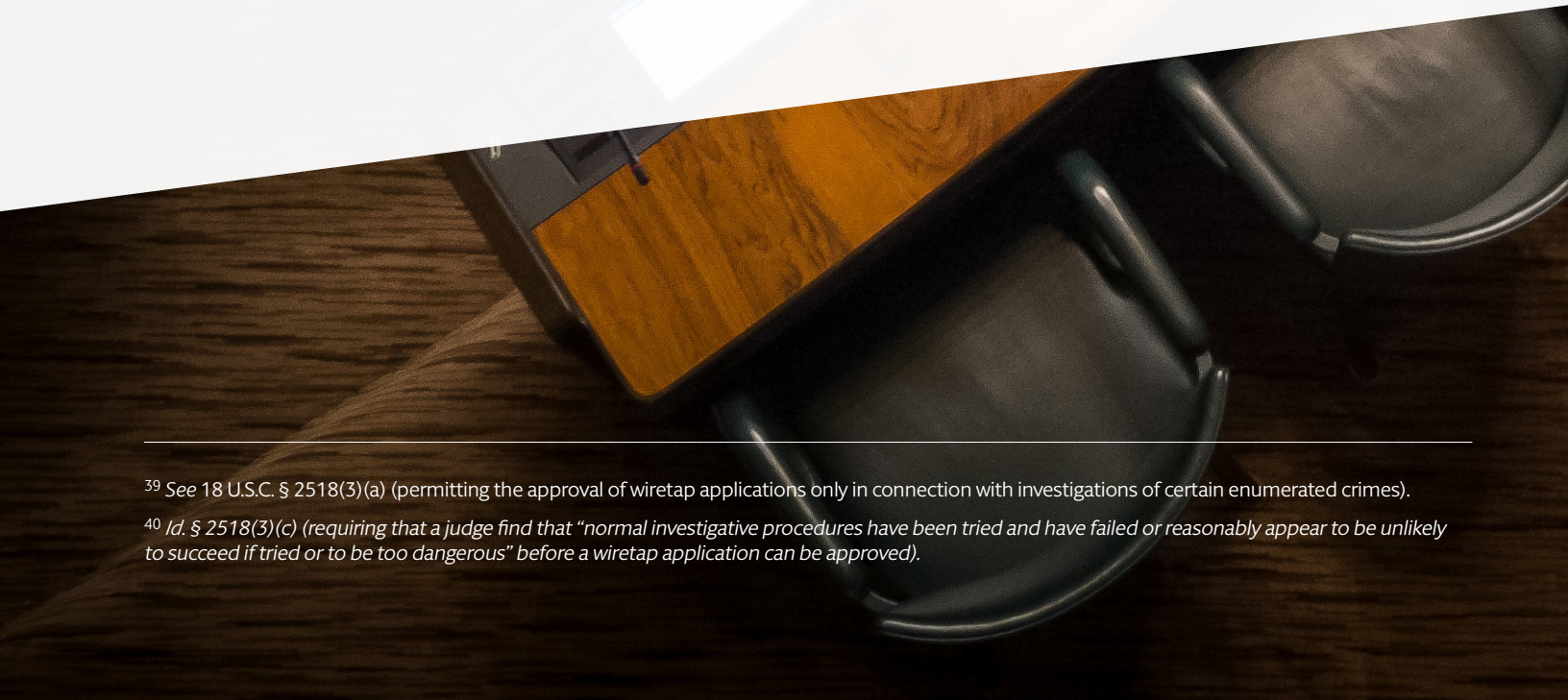
But beyond the SCA, Congress has imposed stricter requirements on specific types of searches. For example, the Wiretap Act allows U.S. law enforcement to engage in wiretapping and electronic eavesdropping, but only in connection with the investigation of certain enumerated crimes.[39] Furthermore, the Wiretap Act requires that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved.[40]

The CLOUD Act does not change the fundamental structure – let alone reduce the substantive data protections – of the Wiretap Act or other privacy laws unrelated to the SCA.

G. The five layers of SCA filters must all be satisfied

IIn summary, the SCA as modified by the CLOUD Act incorporates five cumulative layers of filters, all of which must be satisfied.

- The entity targeted must be an RCS or ECS
- The entity targeted must be under the personal jurisdiction of U.S. courts
- The evidence sought must be under the "possession, custody, or control" of the targeted entity
- Law enforcement must follow legal process, including establishing "probable cause" for certain content
- The application of the warrant must not violate the CLOUD Act's statutory comity framework or principles of international comity as expressed in the Société Nationale Industrielle Aérospatiale case



[39] *See* 18 U.S.C. § 2518(3)(a) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes).

[40] *Id. § 2518(3)(c) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous" before a wiretap application can be approved).*

III. The CLOUD Act was adopted in reaction to *Microsoft v. United States*

A. Summary of the *Microsoft* decision

By passing the CLOUD Act, Congress unquestionably intended to nullify the *Microsoft* decision and moot the U.S. Supreme Court's review of the *Microsoft* decision. As discussed below, the weight of precedent shows that *Microsoft* was an anomaly compared to the other federal court decisions that interpreted the SCA.

In *Microsoft*, the U.S. government served an SCA warrant on Microsoft in the United States (Microsoft U.S.) seeking, among other things, the contents of emails held by Microsoft about a particular account holder.[41] Microsoft challenged the production of the emails, arguing that because the SCA did not apply extraterritorially and emails requested by the warrant were stored on Microsoft's servers in Ireland, it could not be compelled to produce them in response to the warrant.[42]

The district court held, and the U.S. government subsequently argued to the 2nd Circuit, that since the court had undisputed jurisdiction over Microsoft U.S., the U.S. government could compel Microsoft U.S. to produce all customer documents to which Microsoft U.S. had access, including the emails in question.[43] The government analogized SCA warrants to subpoenas rather than search warrants, because SCA warrants do not involve collection directly by the government. Rather, SCA warrants are served on the online service provider, which then has the opportunity to comply with or contest the "warrant." Under existing case law, a subpoena served on an entity that is subject to personal jurisdiction in the United States can compel that entity to produce records stored abroad, so long as the records are in the entity's custody or control.[44] Microsoft lost its motion to quash the warrant in the lower court and, upon failing to produce the documents stored in Ireland, was held in civil contempt, leading to the 2nd Circuit appeal.

The 2nd Circuit reversed, agreeing with Microsoft that the SCA did not apply extraterritorially. It based its decision on the "presumption against extraterritoriality," under which U.S. laws do not apply extraterritorially unless expressly specified by Congress to do so, which Congress did not do with respect to the SCA.[45] Moreover, the 2nd Circuit noted that expanding the application of the SCA so that it applied extraterritorially would be contrary to the privacy protections for users of online services that the statute was enacted to create.[46]

The decision surprised many because it cut against the traditional test of "control, not location" under which the critical element in determining whether a search warrant is executable is whether the entity being served "controls" the data, as opposed to the location of the data at the time the demand was served.[47] The 2nd Circuit, however, distinguished cases that applied that test, noting that they were only applicable

---

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

42 *See id.* at 201.

43 *See id.*

44 *See id.* (citing *Matter of Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983)). SCA warrants and subpoenas are the rough equivalents of production orders under Article 18 of the Council of Europe Cybercrime Convention.

45 *See id.* at 210-216.

46 *See id.* at 219-220.

47 *See Marc Rich & Co., A.G.*, 707 F.2d at 667.

to subpoenas and not warrants, and that the types of records subject to those requests were not subject to the heightened privacy protections of the SCA.[48]

Since the *Microsoft* decision was published in July 2016, there have been numerous cases where judges in districts across the country have come to holdings that depart from *Microsoft*. In each of these cases, U.S. Department of Justice attorneys have argued against the holding in *Microsoft*. We summarize several of those cases below.

B. Post-*Microsoft* decisions

By passing the CLOUD Act, Congress unquestionably intended to nullify the *Microsoft* decision and moot the U.S. Supreme Court's review of the *Microsoft* decision. As discussed below, the weight of precedent shows that *Microsoft* was an anomaly compared to the other federal court decisions that interpreted the SCA.

1. Google (Pennsylvania)

Just a week after the 2nd Circuit denied a rehearing in *Microsoft*, a Pennsylvania federal magistrate judge denied a motion by Google to quash a request from the government to compel the production of user communications stored overseas, where the data also was requested under a SCA warrant.[49] In doing so, the magistrate judge considered and expressly rejected the finding of the 2nd Circuit in *Microsoft*, which was not binding on the Pennsylvania court.

In distinguishing *Microsoft*, the judge stated that the case should not turn on the extraterritoriality of the SCA, but rather on whether the government's request would constitute a Fourth Amendment "search or seizure," and where that action would take place.[50] Considering Fourth Amendment jurisprudence, the judge held that transferring data from servers located overseas to Google in California did not amount to a Fourth Amendment seizure because it did not interfere with account holders' possessory interest in their data, as evidenced by the fact that Google regularly processes such transfers in the course of business. Therefore, the judge held, the request was essentially a request for data held in the United States, avoiding the question of extraterritoriality.[51]

2. Yahoo (Wisconsin)

In late February 2017, a Wisconsin federal magistrate judge also rejected *Microsoft* in requiring Yahoo to comply with an SCA warrant for data stored overseas. The judge refused to apply any extraterritorial limitation on the SCA, going so far as to state that orders under the SCA may be termed "warrants" but do not raise privacy concerns that merit the protections typically afforded a search warrant under the Fourth Amendment. The judge applied the "control, not location" test and stated that under that test, a request for information stored overseas should be considered as a domestic request would be so long as the information is within the custody or control of the U.S. recipient.[52] He went further to state that "[i]f that service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to disclose, consistent with the SCA, that which it can access and deliver within the United States."[53]

---

[48] *See Microsoft*, 829 F.3d at 215-6.

[49] *See In re Search Warrant No. 16-960-M-01 to Google*, 232 F.Supp.3d 708, 709 (E.D. Pa. 2017).

[50] *See* Orin Kerr, *Google Must Turn Over Foreign-Stored Emails Pursuant to a Warrant, Court Rules*, Washington Post (3 Feb. 2017), found here.

[51] *See In re Search Warrant No. 16-960-M-01 to Google*, 232 F.Supp.3d at 719-720.

[52] *See In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo*, No. 2:17-mj-1234-WED, at *7 (E.D. Wis. 21 Feb. 2017).

[53] *See id.*

3. Yahoo (Florida)

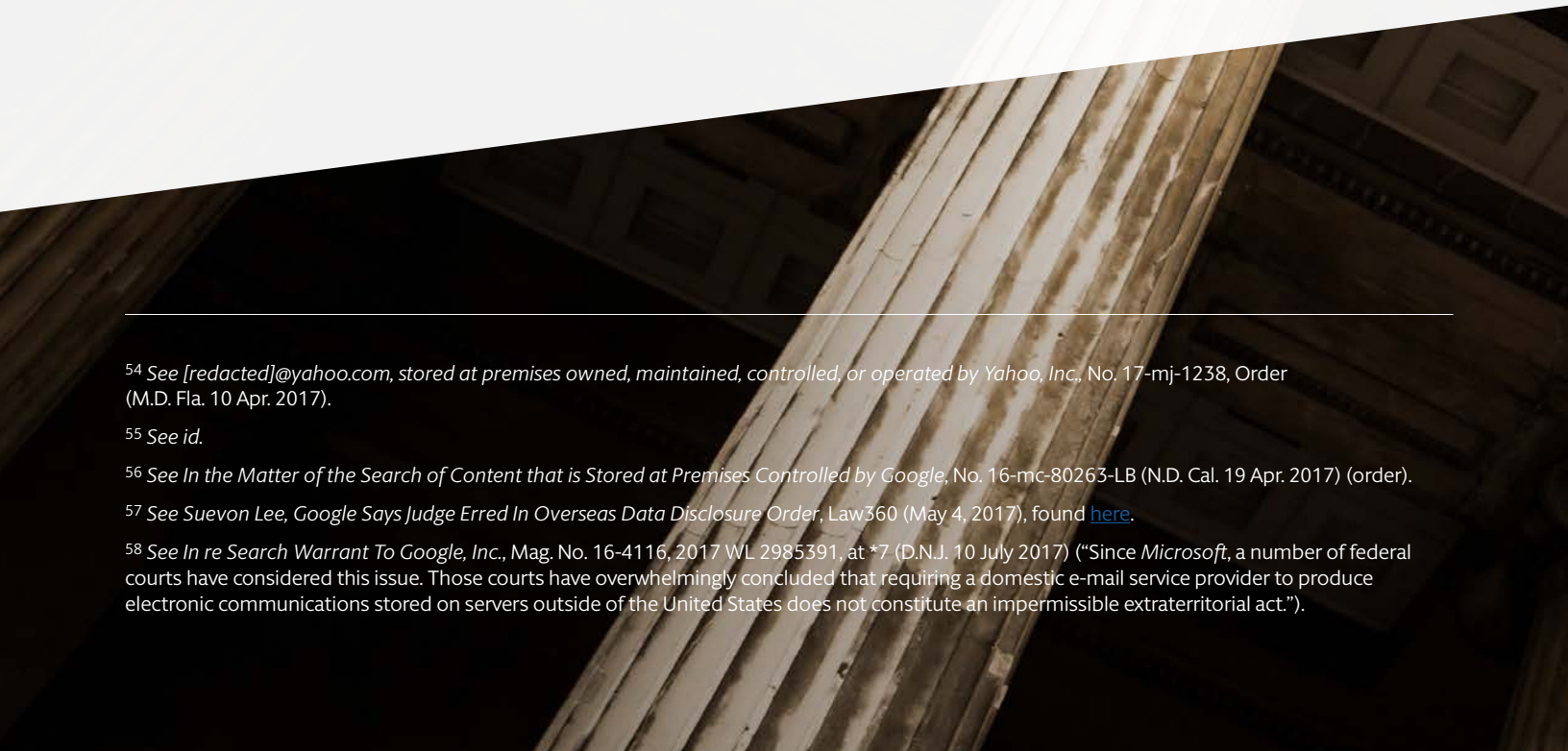
In a decision on 10 April 2017, a federal judge that previously had followed the 2nd Circuit's reasoning in *Microsoft* reversed course, determining that the Pennsylvania (Google) and Wisconsin (Yahoo) cases were more persuasive.[54] In considering another SCA warrant issued to Yahoo, the Florida federal magistrate judge explained that the SCA gives the court personal jurisdiction over the ECS, agreeing that an SCA warrant is more like a subpoena than a traditional warrant.[55] He held that the requirements within the SCA that the government must make a certain showing to a judge before being able to compel the production of documents from a service provider – such as probable cause when seeking an SCA warrant – were adequate to balance any privacy concerns.

4. Google (California)

Barely a week after the Yahoo decision in Florida, a Northern District of California magistrate judge held that Google must produce information held on servers abroad in response to an SCA warrant, also rejecting the decision in *Microsoft* in favor of the logic of the Wisconsin (Yahoo) and Pennsylvania (Google) cases.[56] Google appealed this decision on 3 May 2017.[57]

C. Part 1 of the CLOUD Act Is consistent with virtually all prior U.S. court decisions

The notion that Part 1 of the CLOUD Act represents a major change in the SCA assumes that *Microsoft* had been the settled, well-established interpretation of the SCA for many years. But it was not. Tellingly, the overwhelming number of subsequent cases in other districts have not followed the *Microsoft* ruling or found its reasoning persuasive.[58] By passing the CLOUD Act, Congress rejected *Microsoft* and effectively determined that the overwhelming number of decisions decided contrary to *Microsoft* represents the proper reading of the SCA. Part of the rationale behind the CLOUD Act is that in criminal investigations, criminal suspects should not have an easy way to remove evidence from the jurisdiction of courts and prosecutors. Instead, courts should apply a flexible "possession, custody, or control" standard that is surrounded by robust procedural and human rights safeguards to protect against prosecutorial or court overreaching.



[54] *See [redacted]@yahoo.com, stored at premises owned, maintained, controlled, or operated by Yahoo, Inc.*, No. 17-mj-1238, Order (M.D. Fla. 10 Apr. 2017).

[55] *See id.*

[56] *See In the Matter of the Search of Content that is Stored at Premises Controlled by Google*, No. 16-mc-80263-LB (N.D. Cal. 19 Apr. 2017) (order).

[57] *See* Suevon Lee, *Google Says Judge Erred In Overseas Data Disclosure Order*, Law360 (May 4, 2017), found here.

[58] *See In re Search Warrant To Google, Inc.*, Mag. No. 16-4116, 2017 WL 2985391, at *7 (D.N.J. 10 July 2017) ("Since *Microsoft*, a number of federal courts have considered this issue. Those courts have overwhelmingly concluded that requiring a domestic e-mail service provider to produce electronic communications stored on servers outside of the United States does not constitute an impermissible extraterritorial act.").

IV. International Law, the GDPR and the Budapest Convention

A. International law

Based on the U.N. Charter, principles of international law prohibit a sovereign nation from interfering with the sovereignty of other nations. These principles are well described in the European Commission's amicus brief in the *Microsoft* case:

> "Any domestic law that creates cross-border obligations – whether enacted by the United States, the European Union, or another state – should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity."[59]

The case law of the United States and the European Union both emphasize that laws should be interpreted so as to avoid unreasonable interference with the sovereign authority of other nations. In concrete terms, that doctrine requires judges applying law enforcement statutes, both in the European Union and in the United States, to consider conflicts of law and to avoid them whenever possible. The U.S. Supreme Court articulated the common-law international comity test in Société Nationale Industrielle Aerospatiale,[60] which U.S. courts still apply when dealing with international data requests. The balancing required to minimize conflicts of law is routinely done in cases involving international discovery, or in cases involving EU authorities' request for data located in the United States. In matters of data requests, international law does not impose a bright-line principle that authorities in one state can never access data located in another state without going through international conventions.

A good example of that flexible principle is Article 57-1 of the French Code of Criminal Procedure, which allows police and judges to issue orders requiring access to data stored outside of France as long as there exists an authorized access point in France and the requisition would not violate international law.[61] The French Supreme Court also held that the location of the data does not matter

[59] Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, *United States v. Microsoft* (No. 17-2), 2017 WL 6383224, at *5 (13 Dec. 2017).

[60] *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).

[61] Code de Procédure Pénale [C. Pr. Pén.] [Criminal Procedure Code] art. 57-1 (Fr.).

with regard to searches for documents in the context of tax investigations.[62]

Naturally, if a U.S. judge were to interpret the notion of "control" in an extensive manner that manifestly conflicts with the laws and sovereignty of other nations, a given SCA warrant could violate international law. In this case, the party affected by the order could challenge the order on the basis of violation of principles of international comity, just as a party can challenge the scope of civil discovery orders issued by U.S. judges. The success of such a challenge would depend on the facts and the application of a balancing test by the U.S. judge. The CLOUD Act has changed nothing in this analysis.

To reduce legal uncertainty and expedite international data requests, Part 2 of the CLOUD Act foresees the adoption of EAs between the United States and other countries. Even in the absence of an EA, however, the CLOUD Act expressly preserves the right of a provider to challenge an SCA warrant under "common law ... comity analysis." Under that common-law comity analysis, courts may look to the Société Nationale Industrielle Aerospatiale factors: (1) the importance of the information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means to obtain the information; and (5) the U.S. and foreign interests at stake.[63] Based on the totality of these factors, a court may modify or quash a warrant.

In short, non-U.S. persons have more than one legal basis to challenge an SCA warrant for the content of their data, and the CLOUD Act creates another specific, statutory mechanism to consider international privacy interests.

B. The CLOUD Act and GDPR

Article 48 of the GDPR was adopted specifically to address disclosures required by non-EU jurisdictions. Recital 115 of the GDPR warns that "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 ensure in the Union by this Regulation."[64] Article 48, meanwhile, specifies that treaties, such as MLATs, are the preferred option for law enforcement requests for data involving EU data controllers or processors:

> "Any judgment of a court or tribunal and any decision of an administrative authority or 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, without prejudice to other grounds for transfer."[65]

[62] Cour de cassation [Cass.] [supreme court for judicial matters] com., 26 Feb. 2013, Bull. civ. IV, No. 32 (Fr.).

[63] *Société Nationale Industrielle Aérospatiale*, 482 U.S. at 544 n.28 (1987); *see* Restatement (Third) of the Foreign Relations Law of the United States § 442.

[64] Council Regulation 2016/679, 2016 O.J. (L 119) (GDPR), recital 115.

[65] *Id.* article 48.

Despite its preference for MLATs and other treaties, Article 48 states that the use of treaties is "without prejudice to other grounds for transfer" in Chapter 5 of the GDPR. As Article 49(e) makes clear, these "other grounds" include transfers "necessary for important reasons of public interest,"[66] along with transfers "necessary for the establishment, exercise or defence of legal claims."[67] The European Data Protection Board has indicated that the exception under Article 49(1)(e) covers a range of activities for example, in the context of a criminal or administrative investigation in a third country.[68] Both of these grounds require a balancing of the rights and interests at stake and the implementation of safeguards to protect the rights and freedoms of individuals.

A combined reading of Article 48 and 49 of the GDPR suggests that communication of data pursuant to a warrant issued under the SCA is not necessarily, and certainly not automatically, a violation of the GDPR. An MLAT or EA should be used where possible, but if sufficient safeguards are implemented, Article 49 of the GDPR permits communication without use of a treaty mechanism.

C. Council of Europe Cybercrime Convention

The Council of Europe Convention on Cybercrime establishes an international framework to harmonize the procedure and substantive laws governing computer crimes.[69] Enacted in 2001, the Cybercrime Convention requires signatories – which encompass more than 50 nations, including the United States and EU member states – to criminalize certain types of cybercrimes, implement standardized procedures for lawful preservation and disclosure of related stored data, and cooperate with other signatories on cross-border law enforcement requests. The SCA as clarified by the CLOUD Act is fully consistent with Article 18(1) of the Cybercrime Convention, which requires signatories to adopt measures that would allow its law enforcement authorities to reach data in two situations. First, local law enforcement can reach "computer data" (including content) of a person in the country if that person has "possession or control" over that data.[70] Second, local law enforcement can obtain noncontent "subscriber data" that is within a service provider's "possession or control" if the provider offers services in the territory.[71]

---

[66] *Id.* article 49(1)(d).

[67] *Id.* article 49(1)(e).

[68] European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, 25 May 2018, at 11.

[69] Council of Europe Convention on Cybercrime 23 Nov. 2001, S. Treaty Doc. No. 11, 108th Cong., 1st Sess. (2003), 2296 U.N.T.S. 167 (Cybercrime Convention); *see also* Council of Europe, *Explanatory Report to the Convention on Cybercrime*, ETS No. 185 (23 Nov. 2001) (Explanatory Report).

[70] Cybercrime Convention Art. 18.1(a).

[71] *Id.* at Art. 18.1(b).

The use of "possession or control" under the Cybercrime Convention generally corresponds to the concept of "possession, custody, or control" under U.S. law. For a service provider, the Cybercrime Convention defines "possession or control" to mean "subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."[72] Thus, like the CLOUD Act, the Cybercrime Convention requires providers to disclose subscriber data in their possession and control, even when the data is held somewhere else.

Finally, the European Union has proposed a new e-evidence legislative proposal.[73] The Council of Europe, meanwhile, is drafting a second protocol to the Cybercrime Convention.[74] Both initiatives would permit local law enforcement access to data stored outside their jurisdiction while establishing due process safeguards and minimizing impacts on human rights. These measures are consciously designed to reconcile interests surrounding state sovereignty, law enforcement, and user privacy.

In short, under the European Union's emerging framework, the physical location of the data is increasingly irrelevant, as with the CLOUD Act. According to the European Commission's frequently asked questions (FAQ), "[t]he Regulation departs from data storage as the determining factor for jurisdiction, and rather requires that the requested data is (1) needed for a criminal proceeding for which the issuing authority is competent and (2) related to services of a provider offering services in the Union. If this is the case, the data must be preserved and produced, irrespective of the place of data storage."[75] The e-evidence regulation would apply a flexible approach to data location, surrounded by robust procedural and human rights safeguards.

---

[72] Explanatory Report ¶ 173.

[73] European Commission, *E-evidence - cross-border access to electronic evidence*, found here.

[74] *Council of Europe, T-CY Drafting Group*, found here.

[75] European Commission, *Frequently Asked Questions: New EU rules to obtain electronic evidence* (17 Apr., 2018), found here.

V. Conclusion

Fears about the CLOUD Act's effect on global web services have been overstated and are often based on mistaken assumptions. Part 1 of the CLOUD Act confirms the "control, not location" interpretation of the SCA that nearly all U.S. courts have applied for many years. It does not give the U.S. government sweeping new power; instead, it largely clarifies the legal consensus that predated the *Microsoft* case.

Nor does Part 1 of the CLOUD Act deprive EU citizens or service providers of meaningful legal recourse. The U.S. Constitution, SCA, and the CLOUD Act itself contain numerous procedural and substantive legal and practical safeguards to mitigate the risk of overbroad surveillance, and these sources of U.S. law are equivalent to the level of safeguards afforded under EU laws and treaties.

Any warrant issued under the SCA for a criminal investigation must satisfy five cumulative filters.

- The entity targeted must be an RCS or ECS
- The entity targeted must be under the personal jurisdiction of U.S. courts
- The evidence sought must be under the "possession, custody, or control" of the targeted entity
- Law enforcement must follow legal process, including establishing "probable cause" for certain content
- The application of the warrant must not violate principles of international comity as expressed in the Société Nationale Industrielle Aérospatiale case

The "possession, custody, or control" test is similar to the standard applied under the Council of Europe Cybercrime Convention, and the proposed EU e-evidence regulation. As the emerging global consensus makes clear, the physical location of data is increasingly unlikely to be a determining factor going forward.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

Associated offices*

www.hoganlovells.com