Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act

Justin Hemmings,* Sreenidhi Srinivasan** & Peter Swire***

Introduction

The U.S. entered into its first Mutual Legal Assistance Treaty (MLAT) with Switzerland in 1977 in response to law enforcement's frustration with knowing the location of evidence but being unable to reach it.[1] At that time, criminal organizations were taking advantage of Swiss banking secrecy laws to hide money and transactions, frustrating U.S. law enforcement investigations.[2] Over time, more countries entered into MLATs as a means of accessing evidence located outside of a country's physical jurisdiction. Today, however, the sheer amount of electronic evidence has made ubiquitous the need for law enforcement to access this kind of evidence stored outside of their physical jurisdiction. It was in this context that the U.S. Congress passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) in 2018.

When the CLOUD Act came into law, it mooted the *Microsoft Ireland* case then pending in the U.S. Supreme Court, but left stakeholders confused as to the current state of play for accessing electronic evidence stored outside the U.S.[3] The CLOUD Act codified that the U.S. government has the power to order the production of electronic evidence from U.S. service providers "regardless of whether such [evidence] is located within or outside of the United States."[4]

---

* Justin Hemmings is a research faculty member at the Georgia Tech Scheller College of Business. The authors particularly thank Mona Giacometti for her assistance with the article, and particularly for her expert assistance on issues of Belgian law. The authors also thank those who provided comments on earlier drafts of this paper at the Privacy Law Scholars Conference and the Third Way Cyber Enforcement Workshop.

** At the time of drafting this article, Sreenidhi Srinivasan was a research faculty member at the Georgia Tech Scheller College of Business. She is now Senior Associate at Ikigai Law, a law firm based in New Delhi.

*** Peter Swire is the Elizabeth and Tommy Chair of Law and Ethics, in the Georgia Tech Scheller College of Business; Senior Counsel, Alston & Bird LLP. Our thanks for funding for this research from an award for Swire's Andrew Carnegie Fellowship, the Cross-Border Data Forum, the Georgia Tech Institute of Information Security and Privacy, and the Hewlett Foundation Cyber Program.

1. *See* William W. Park, *Legal Policy Conflicts in International Banking*, 50 Ohio St. L.J. 1067, 1096 (1989).

2. *See id.*

3. This paper will focus on Sections 103 and 104 of the Cloud Act which mooted the *Microsoft Ireland* case by amending the Electronic Communications Privacy Act of 1986. *See* Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, § 3, 132 Stat. 350. For further discussion of multiple legal issues arising under the Cloud Act, see Peter Swire & Jennifer Daskal, *Frequently Asked Questions about the U.S. CLOUD Act*, Cross-Border Data Forum (Apr. 16, 2019), https://perma.cc/V2KY-NAMK.

4. 18 U.S.C. § 2713 (2012).

Instead of location, the CLOUD Act establishes that the provider's "possession, custody, or control" is the determining factor for whether the service provider must provide the specified evidence.[5] Yet, the Act does not define "possession, custody, or control" of electronic evidence. This article addresses that task, defining that key term.

Without a clear definition, some stakeholders, particularly in Europe, have understandably raised concerns about the scope of the U.S. government's asserted authority under the CLOUD Act. Member of European Parliament Sophie in 't Veld wrote that "[w]ith the CLOUD Act, the Americans have direct access to European databases with data on European citizens."[6] The French government has expressed concern that the CLOUD Act is harmful to its "digital sovereignty," and French private sector actors have accused the U.S. government of enabling the U.S. government to engage in economic espionage targeting foreign companies.[7] While some of these concerns misunderstand the CLOUD Act's interaction with existing U.S. law,[8] the lack of a clear definition of "possession, custody, or control" has engendered confusion.

Law enforcement, both inside and outside the U.S., would benefit from a clear understanding of "possession, custody, or control." First, for cautious investigators, an unclear definition means a higher likelihood they will rely on a conservative interpretation of the phrase. Doing so means they may miss out on collecting evidence to which they are entitled, or delaying their access to such evidence by instead relying on a more well-trodden but time-consuming process, like a formal MLAT request. Second, more risk-accepting investigators may take an aggressive interpretation of the phrase to collect more evidence than they would otherwise be entitled to demand. Finally, a clearer definition would enable more effective sharing of investigative responsibilities. Both U.S. and foreign law enforcement could cooperate more effectively on joint and parallel investigations with a clearer understanding of what U.S. law enforcement can and cannot do with its powers under the CLOUD Act.

To understand how courts may analyze whether a company has "possession, custody, or control" over data, we introduce a new visualization tool, shown below as *Figure 1*.

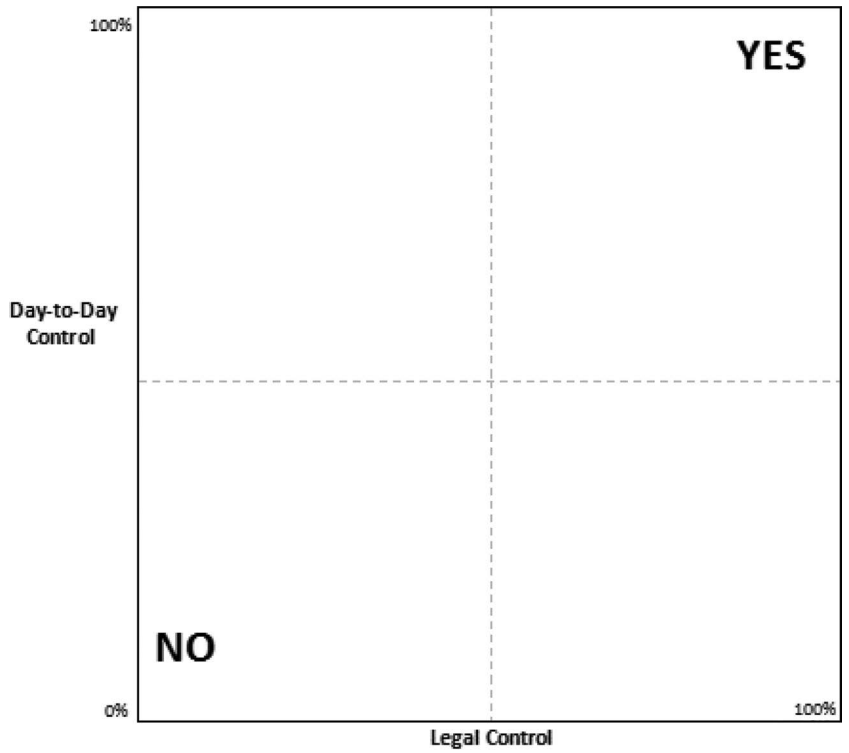
5. *Id.*

6. *See Long arm of American Law? Not in Europe!*, STERK EUROPA SOPHIE (Feb. 5, 2019), https://perma.cc/A6ZH-M36T/.

7. *See* Justin Hemmings & Nathan Swire, *The Cloud Act Is Not a Tool for Theft of Trade Secrets*, LAWFARE BLOG (Apr. 23, 2019, 8:00 AM), https://perma.cc/8EMP-UKZM.

8. *See id.* (explaining why U.S. normative and diplomatic interests, criminal procedure law, Presidential Policy Directive 28, and the Economic Espionage Act make it highly unlikely that the Cloud Act could be used to conduct economic espionage).

Figure 1:
Describing Where Courts Find Possession, Custody, or Control

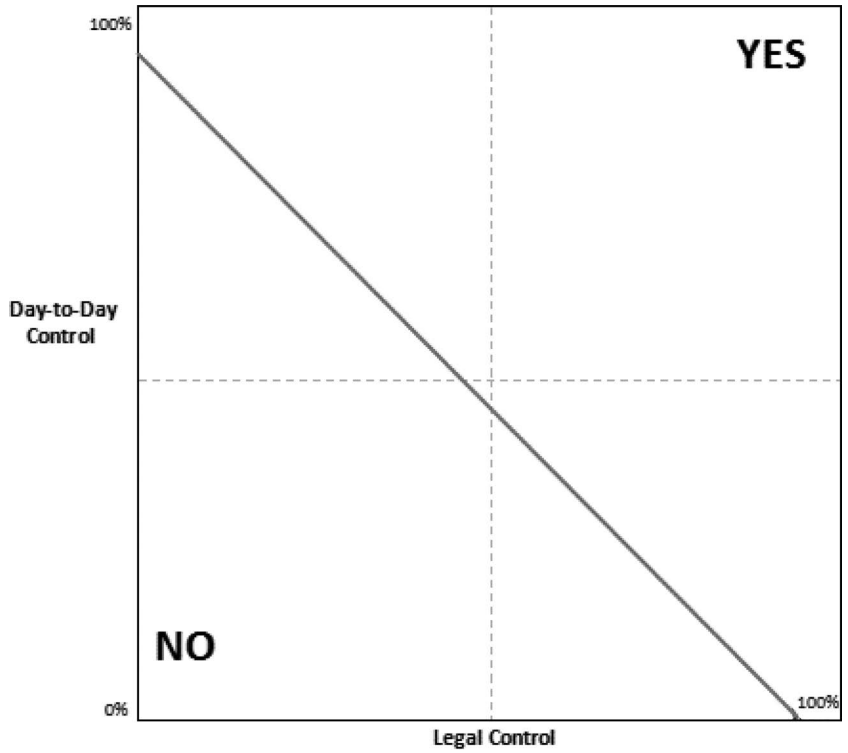


The graph has two variables: the amount of legal control the entity receiving the legal process has over the evidence and the amount of day-to-day control the entity exerts over the evidence. Where the entity has 100% legal and day-to-day control of evidence, courts would almost certainly require production of the evidence sought. Likewise, where the entity has 0% legal and day-to-day-to control, courts are unlikely to require production and the government would be required to issue process on an entity that more clearly has "possession, custody, or control" over the evidence sought.

While we do not expect courts to make precise findings of the percentage of legal and day-to-day control, we suggest that this graph conceptualizes key aspects of how courts interpret the doctrine. Relying on the two axes of "day-to-day" and "legal" control, one can approximate a line of where courts tend to find possession, custody, or control, in some cases even where the corporate entity receiving the request does not hold the evidence. Figure 2 illustrates one such hypothetical line, although we emphasize that we are not trying to reach legal conclusions about what percentage of control on each axis leads courts to find possession, custody, or control. In Figure 2, a point up and to the right of the line would result in a decision to find such control,

while a point below and to the left of the line would not. The line in Figure 2 describes doctrine in which 100% legal control or 100% factual control would require production of the information, which is the most likely outcome from the case law that we analyze below.

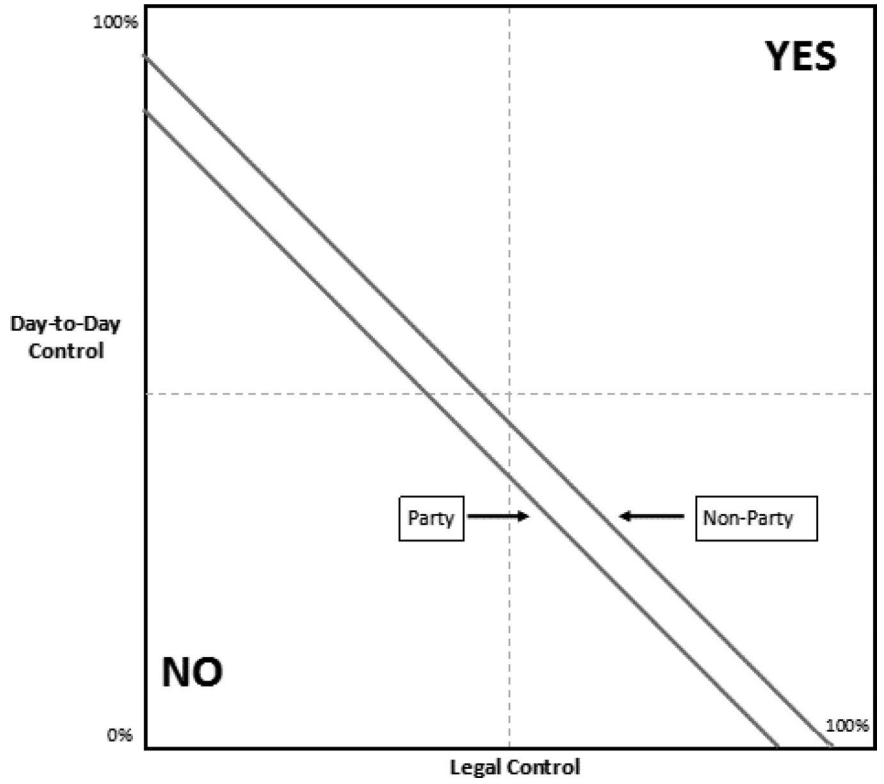
Figure 2:
Line Roughly Describing Where Courts Find Possession, Custody, or Control



In addition to "day-to-day" and legal control, courts will often look to whether the targeted entity is a party to the case at hand. Generally speaking, courts are more likely to require production from a party to the case, as a party is incentivized to avoid producing evidence that may make it less likely to prevail. Conversely, a non-party has no such direct interest in the case and, therefore, has no inherent incentive to avoid production. Figure 3 shows the effect of whether the request is to a party or a non-party: a party is generally required to produce evidence in a greater range of situations than a non-party.

We suggest that Figure 3 offers a concise summary of our research on where courts require an entity to respond to a government request.

Figure 3:
Effect of Party and Non-Party for Where Courts Find Possession, Custody, or Control



One could apply this graph in two ways. In the first method, a holistic analysis of the particular facts of the individual case would result in two values: the total percentage of legal control and of day-to-day control the entity exerts over the data. Alternatively, for each key fact about the entity's interaction with the data, one could determine how much legal and day-to-day control that individual fact demonstrates, and plot each fact accordingly. There would then be either one point, or a series of points, plotted on the chart, depending on the method used.

Again, we stress that the graph is intended as an aid to understanding – we do not intend Figure 3 to portray the precise location of the x and y intercept or the precise shape or slope of each line. Instead, we suggest that this graph illuminates how courts have interpreted the meaning of "control" in the cases we review in this article.

This article examines the current lack of clarity about the meaning of "possession, custody or control" and suggests how existing case law interpreting this exact phrase in other legal contexts can inform U.S. judges in interpreting the phrase's meaning in the CLOUD Act. Part I examines whether the use of this standard in the CLOUD Act expanded the DOJ's previous power to require the production of electronic evidence from U.S.-based service providers. This part

reviews the *Bank of Nova Scotia* line of cases and lower court rulings in *Microsoft Ireland*, as well as the different viewpoints on the scope, prior to the CLOUD Act, of the U.S.'s authority to demand the production of electronic evidence stored outside the U.S. Our conclusion is that the CLOUD Act primarily confirmed the previous judicial interpretations, rather than significantly expanding the authority, which some have claimed.

Part II examines how courts have interpreted the phrase "possession, custody, or control" under the Federal Rules of Civil and Criminal Procedure, and how that jurisprudence might inform future challenges of U.S. authority under the CLOUD Act. The exact phrase is found in Rules 34 and 45 of the Federal Rules of Civil Procedure and Rule 16 of the Federal Rules of Criminal Procedure. These rules consider when parties and non-parties to litigation, including the U.S. government, can be required to turn over information and documents. This section will then look closely at four additional implications from existing jurisprudence:

1. How the courts have treated different types of international corporate structures and how the location and nature of parent, subsidiary, or affiliated corporations affects the determination of "possession, custody, or control;"
2. How the interpretation of "possession, custody, or control" differs as applied to parties and non-parties, and which more closely resembles the position of an electronic service provider under the CLOUD Act;
3. How the courts decide if and when to "pierce the corporate veil" to assert "possession, custody, or control" of information, and how to differentiate the legal and policy context of "piercing the veil" in this context; and
4. Why an entity's "control" of data for purposes of the CLOUD Act is different from the designation of a "data controller" under the European General Data Protection Regulation (GDPR).

Finally, this part will attempt to synthesize these different interpretations and nuances of "possession, custody, or control" and how they might apply to the CLOUD Act in light of its particular policy implications.

Part III will review concepts similar to the "possession, custody, or control" standard in other nations. Specifically, this section will review Belgian law, based on prominent recent cases decided by Belgian courts. The Belgian courts have required the production of evidence stored by electronic service providers outside of Belgium in two cases, involving Yahoo! and Skype. This section will also compare how the U.S. and Belgian courts have approached the issue of when to require the production of evidence in these types of cases, highlighting similarities and differences.

In short, this Article seeks to clarify how courts have previously interpreted the meaning of "possession, custody, or control" in other contexts and how that may influence future interpretations of the phrase under the CLOUD Act. This Article seeks to outline key factors that courts will likely weigh in their analysis of this

pivotal phrase and to highlight particular issues that are likely to arise in this context.

I. BACKGROUND OF THE CLOUD ACT: THE *BANK OF NOVA SCOTIA* DOCTRINE

With increasing data flows across borders, law enforcement agencies have faced severe challenges in accessing data located in other jurisdictions, testing the reach of local laws and their ability to require production of evidence stored abroad.[9] Even before the CLOUD Act, U.S. courts have required individuals and entities that are subject to U.S. jurisdiction to produce evidence within their possession or control regardless of where the data is physically stored.[10] This principle is reflected in a line of cases from the 1980s involving the Bank of Nova Scotia, in which subpoenas were served on U.S. branches of the bank to produce records that were located with its offshore branches.[11] The justification for this approach, commonly known as the "Bank of Nova Scotia doctrine," was that such subpoenas were necessary to be able to trace the flow of money outside the U.S. in criminal investigations.[12] In the Department of Justice's view, the CLOUD Act only makes explicit the "long-established U.S. and international principle" that a company that is subject to a country's jurisdiction can be required to produce data within its custody and control.[13]

The Bank of Nova Scotia doctrine was discussed at various stages of *Microsoft Ireland*,[14] a case that dealt with the scope of the U.S. government's powers to compel production of electronic communications stored overseas. The case focused on the application of the Stored Communication Act (SCA) [15] – the

9. *See* Jennifer C. Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015); Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687 (2017); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L.R. 729 (2016); Peter Swire, *Why Cross-Border Requests for Data Will Keep Becoming More Important*, LAWFARE BLOG (May 23, 2017, 10:00 AM), https://perma.cc/U8EW-UZSS.

10. U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL, § 279(B), https://perma.cc/TZ5J-U2JC; U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y.

11. *See In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985); *In re* Grand Jury Proceedings (Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983).

12. *See* Bank of Nova Scotia, 740 F.2d at 817.

13. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y; Richard W. Downing, Deputy Assistant Attorney General, Dep't of Justice, Delivers Remarks at the Academy of European Law Conference on "Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety" (Apr. 5, 2009), https://perma.cc/E68J-65J6 ("It is well established that a company present in our territory is subject to a U.S. subpoena for physical records in its possession, custody, or control, and must produce those records, regardless of where they are stored. For decades, the corollary principle – that a provider in our jurisdiction must produce evidence in its control, regardless of where the provider chooses to store the evidence – has been equally settled.").

14. Microsoft Corp. v. United States (In re a Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp.) 829 F.3d 197 (2d Cir. 2016) (An appeal against the Second Circuit ruling was argued before the Supreme Court but was dismissed as moot after passage of the Cloud Act).

15. 18 U.S.C. § 2703 (2010).

portion of the U.S. Electronic Communications Privacy Act (ECPA) that governs law enforcement access to stored electronic communications. In *Microsoft Ireland*, the U.S. Supreme Court was expected to decide whether the SCA applied to communications stored outside the U.S.[16] Before the Supreme Court could rule on the matter, the U.S. Congress passed the CLOUD Act in March 2018. [17] The newly enacted law stated that service providers could be required to disclose the contents of communications within the provider's "possession, custody, or control," regardless of where the communications or other information was located.[18] With the passage of the CLOUD Act, the Supreme Court declared moot the central question of *Microsoft Ireland* – whether the Stored Communication Act would apply overseas.[19]

In this section, we trace the history and context of the decision in *Bank of Nova Scotia* and related rulings. We then discuss the *Microsoft Ireland* case and the scope of the U.S. government's powers to require production of electronic communications stored overseas. The last part of this section discusses the passage of the U.S. CLOUD Act, which mooted the need for a ruling in the *Microsoft Ireland* case by codifying the "possession, custody or control" standard in law.

A. The Bank of Nova Scotia Doctrine and Use of Subpoenas for Compelling Production of Documents Stored Overseas

Courts have upheld the use of subpoenas to compel banks or other businesses to produce records located with their overseas branches. The principle is commonly known as the Bank of Nova Scotia doctrine, following judgments requiring the Bank of Nova Scotia to produce records stored in its overseas branches. In this section, we discuss the case, related judgments, and the context in which courts upheld such subpoenas.

1. The Bank of Nova Scotia Case

In re Grand Jury Proceedings (Bank of Nova Scotia)[20] addressed a narcotics investigation involving customers of the Bank of Nova Scotia (BNS), a Canadian banking corporation with over 1200 branches and offices in several countries. The bank's Miami branch was served with a grand jury subpoena calling for production of financial documents relating to two individuals and three companies from the bank's branches in the Bahamas, Cayman Islands, and Antigua.[21] BNS

16. *See* Andrew Keane Woods, *Primer on Microsoft Ireland, the Supreme Court's Extraterritorial Warrant Case*, LAWFARE BLOG (Oct. 16, 2017, 2:07 PM), https://perma.cc/H3W8-CXF2.

17. 18 U.S.C. § 2523 (2012).

18. *Id.*

19. United States v. Microsoft Corp., 138 S.Ct. 1186 (2018); Amy Howe, *Justices Officially Declare Microsoft Email Case Moot*, SCOTUS BLOG (Apr. 17, 2018), https://perma.cc/8S8G-5X9T.

20. *In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984), *cert. denied*, 469 U.S. 1106 (1985).

21. A grand jury is a group comprising 16-23 persons that examines evidence and decides whether to charge a person in a criminal case. A subpoena is a legal instrument that can be served on a person or an entity to produce documents. Grand juries can serve individuals or corporations with subpoenas for

filed several motions to quash the subpoena on the ground that production of the documents sought was not permitted under foreign laws.[22] The court denied these motions and issued a contempt order against the bank for failing to produce documents in accordance with the subpoena.[23] BNS appealed the order before the Eleventh Circuit Court of Appeals.

The Eleventh Circuit undertook a comity analysis, balancing competing interests in requiring and preventing disclosure, and held that American interests in the documents sought were significant and that the U.S. could serve a local branch with a subpoena for such records.[24] It is useful to note the context in which the court issued the ruling—the information sought through the subpoena concerned transactions of individuals who were the target of a narcotics investigation. That is, the information sought concerned customers of the entity holding the records, similar in that respect to a service provider who holds emails or other records on behalf of its customers. The court highlighted the importance of being able to trace the flow of money to stop the narcotics trade and noted that the Congress and the Executive Branch had been concerned about the use of foreign financial institutions in jurisdictions with strict bank secrecy laws to evade domestic criminal, tax, or regulatory requirements.[25] The court also noted that the interest of American citizens in the privacy of their bank records was reduced

---

production of documents that could aid in deciding whether to indict an individual in connection with a criminal offense. *See* U.S. DEP'T OF JUSTICE, JUSTICE MANUAL, TITLE 9-11.000-GRAND JURY, https://perma.cc/E94S-UGQC (The Justice Manual is a collection of publicly available Department of Justice policies and procedures used to provide internal guidance to the Department of Justice).

22. The bank secrecy law of Cayman Islands required that any person intending to give in evidence, in any proceeding, any confidential information will first have to apply for directions to the Attorney General. *In re* Bank of Nova Scotia, 740 F.2d 817, 833 n.2 (11th Cir. 1984) (quoting Confidential Relationships (Preservation) Law 1979, § 3A(1)-(2) (Cayman Is.)).

23. Under Rule 17(g) of the Federal Rules of Criminal Procedure, a failure by a person to obey a subpoena served upon him or her, without adequate excuse, may be deemed a contempt of the court. FED. R. CRIM. P. 17(g).

24. The Restatement (Second) of Foreign Relations Law of the United States sets out factors to be considered when laws of different states require inconsistent conduct from a person. RESTATEMENT (SECOND) OF FOREIGN RELATIONS L. OF U.S. § 40 (AM. LAW INST. 1965) ("Where two states have jurisdiction to prescribe and enforce rules of law and the rules they may prescribe require inconsistent conduct upon the part of a person, each state is required by international law to consider, in good faith, moderating the exercise of its enforcement jurisdiction, in the light of such factors as:

> (a) vital national interests of each of the states,
> (b) the extent and the nature of the hardship that inconsistent enforcement actions would impose upon the person,
> (c) the extent to which the required conduct is to take place in the territory of the other state,
> (d) the nationality of the person, and
> (e) the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.").

25. Bank of Nova Scotia, 740 F.2d at 817 ("[T]he serious and widespread use of foreign financial institutions, located in jurisdictions with strict laws of secrecy as to bank activity, for the purpose of violating or evading domestic criminal, tax and regulatory enactments.").

when balanced against the interests of their own government in a criminal investigation since certain laws required banks to report those transactions to the U.S.[26]

In addition, the court was guided by the fact that grand juries played a vital role in investigating possible criminal violations and that courts had repeatedly allowed grand juries wide discretion in seeking evidence.[27] Formal processes for cross-border data access, such as letters rogatory, would require a showing of necessity or relevance of the requested documents to the investigation. In the court's view, requiring a grand jury investigation to follow such processes would "frustrate the public's interest in the fair and expeditious administration of the criminal laws."[28]

Congress expressly authorized subpoenas to banks outside the U.S. under the 2001 USA PATRIOT Act.[29] This statute extended the BNS doctrine beyond the bank branches at issue in the BNS case.[30] Now, by statute, the BNS doctrine applies even where the foreign bank merely has a correspondent account in the U.S. A correspondent account is an account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank.[31] The subpoena thus reaches beyond the records held by the bank's own branches, to the records held by a different bank, subject to U.S. jurisdiction, if the foreign bank itself has a qualifying account with that different bank.

In 2016, the DOJ proposed an amendment to further expand these subpoena powers.[32] The proposed amendment would expand DOJ's authority to issue USA PATRIOT Act subpoenas to foreign banks that maintain a correspondent account in the United States to include not only records relating to that account, but also records pertaining to *any* related account at the foreign bank, including records maintained outside the United States, that are the subject of any investigation of a criminal violation of U.S. law or a civil forfeiture action. DOJ supported this expansion since large global financial institutions with U.S. correspondent accounts were processing illicit funds outside the U.S. and since records relevant to a U.S. investigation could be located overseas.[33] Congress to date has not adopted that proposed expansion of subpoena powers.

---

26. Banks were required to report pursuant to 31 U.S.C. § 1121 (1976) and 31 C.F.R. § 103.24 (1979).

27. Bank of Nova Scotia, 740 F.2d at 825 (citing U.S. v. Dionision, 410 U.S. 1 (1973)).

28. *Id*. at 825.

29. 31 U.S.C. § 5318(k)(3) (2012); USA PATRIOT Act, Pub. L. No. 107-56, § 319(b), 115 Stat. 272, 312 (2001).

30. 31 U.S.C. § 5318(k)(3)(A)(i) (2012) ("The Secretary of the Treasury or the Attorney General may issue a summons or subpoena to any foreign bank that maintains a correspondent account in the United States and request records related to such correspondent account, including records maintained outside of the United States relating to the deposit of funds into the foreign bank.").

31. 31 C.F.R. § 1010.605(c) (2018).

32. This provision was part of anti-corruption legislative proposals submitted by the DOJ to Congress in connection with illegal proceeds of transnational corruption. U.S. DEP'T OF JUSTICE, ANTI-CORRUPTION LEGISLATIVE PROPOSALS ON TRANSNATIONAL AND PUBLIC CORRUPTION (2016), https://perma.cc/AC5T-88TV.

33. *Id*.

2. The Marc Rich Case and the "Control" Test

While the decision in *Bank of Nova Scotia* and the PATRIOT Act provision did not refer to "control," other cases noted and relied on the principle that the relevant test in determining whether a subpoena can be served is control and not location.[34] The Second Circuit opinion in *Marc Rich v. United States*,[35] which featured heavily in the *Microsoft Ireland* case, relied on this principle. It is also useful to note that in *Bank of Nova Scotia*, the bank was a third party whose records were called for to investigate its customers' accounts.[36] In *Marc Rich*, however, the corporation itself was the target of the investigation. As discussed below, courts have generally found a greater scope to access records of a party to the litigation, compared to somewhat narrower scope for records held by a non-party, such as a bank or online service provider holding customer records.[37]

Marc Rich was a Swiss commodities trading corporation, with its principal office in Switzerland and forty branches in several countries around the world. Marc Rich had a wholly owned subsidiary in New York – Marc Rich International. In March 1982, a federal grand jury was investigating a tax evasion scheme involving Marc Rich, the New York subsidiary, and the principals of each company. A grand jury subpoena addressed to the Swiss corporation was served on its New York subsidiary for production of business records relating to certain crude oil transactions.[38] Marc Rich moved to quash the subpoena on the ground that it was not subject to the personal jurisdiction of the court and that Swiss law prohibited the production of the materials demanded. A district court denied the motion to quash and held Marc Rich in contempt for failing to produce the documents.

On appeal, the Second Circuit upheld the subpoena, holding that personal jurisdiction existed over the Swiss corporation and that Swiss law did not operate as a bar to production of the documents. The court found personal jurisdiction over Marc Rich noting that if the corporation had violated tax laws, it was in conjunction with its wholly-owned subsidiary in New York and that parts of the conspiratorial acts occurred within the United States.[39] The Second Circuit held that a

34. *E.g., In re* Marc Rich & Co., A.G., 707 F.2d 663 (2d Cir. 1983), *cert denied*, 463 U.S. 1215 (1983) (citing *In re* Canadian Intern. Paper Co., 72 F. Supp. 1013, 1020 (S.D.N.Y. 1947)).

35. *Id.*

36. *But see In re* Sealed Case, 825 F.2d 494 (D.C. Cir. 1987) (finding that no action should be brought against the bank after taking into account circumstances including the fact that the bank was a third party not accused of wrongdoing and acted in good faith in trying to comply with the subpoena).

37. *See* discussion *infra* Part II.

38. Prior to that, another subpoena had been served on the New York subsidiary for its records which was complied with.

39. *See* Marc Rich, 707 F.2d at 668 ("If appellant did violate the United States tax laws, a question whose answer must await the possible return of an indictment, that violation occurred in cooperation with appellant's wholly-owned subsidiary, Marc Rich & Co. International, Ltd., which is authorized to do business in New York State and does so. Moreover, two of the five members of appellant's board of directors, who are also on the board of Marc Rich & Co. International, are residents of the United States. At least one of these directors is alleged to have been directly involved in the scheme to divert the taxable income of International. If, in fact, there was a conspiracy among all of these parties to evade the

corporation subject to the personal jurisdiction of the grand jury could not resist production on the ground that the documents were located abroad.

A grand jury could, thus, subpoena the corporation to obtain its records, even when the records were located overseas.[40] In reaching this conclusion, the court relied on the principle that the test for production of documents was control, not location.[41] This principle and the *Marc Rich* case featured heavily in the DOJ's arguments before the Second Circuit and the Supreme Court in the *Microsoft Ireland* case.[42]

3. The DOJ's View on the "Control" Test and Use of Subpoenas to Compel Production of Documents Stored Overseas

The DOJ has consistently stated that the control test – the idea that a company subject to U.S. jurisdiction can be required to produce data within its custody or control, regardless of where it chooses to store that data at any point in time – has been an established principle of U.S. and foreign law.[43]

In its Criminal Resource Manual,[44] the DOJ has discussed the use of Bank of Nova Scotia subpoenas and noted the line of cases where courts have required that banks doing business in the U.S. turn over records held by their branches in a foreign country, even when producing the records would violate the foreign country's laws.[45] While stating its view that the legal authority exists, the DOJ cautions against excessive use of such subpoenas in cases where foreign laws block production, since foreign governments strongly object to such subpoenas. Specifically, the DOJ requires federal prosecutors to obtain written approval through the Office of International Affairs (OIA) before issuing these

---

tax laws, both the conspiracy and at least some of the conspiratorial acts occurred in the United States. *See* Melia v. United States*, supra*, 667 F.2d [300,] 303–04 [(2d Cir., 1981)]. Under such circumstances, service of a subpoena upon appellant's officers within the territorial boundaries of the United States would be sufficient to warrant judicial enforcement of the grand jury's subpoena. 1 FTC v. Compagnie de Saint-Gobain- Pont-a-Mousson, 636 F.2d 1300, 1324 (D.C.Cir.1980); *In re* Electric & Musical Industries, Ltd., 155 F. Supp. 892 (S.D.N.Y.), *appeal dismissed*, 249 F.2d 308 (2d Cir.1957); *In re* Canadian Int'l Paper Co*., supra*, 72 F. Supp. at 1019–20; Fed. R. Civ. P. 4(d)(3); Fed. R. Crim. P. 17(e)(1).").

40. Subpoenas would not be enforceable if U.S. courts did not exercise personal jurisdiction over the company. *See, e.g.*, *In re* Sealed Case, 832 F.2d 1268, 1272 (D.C. Cir. 1987).

41. *In re* Canadian Int'l Paper Co., 72 F. Supp. 1013, 1019-20 (S.D.N.Y. 1947).

42. *See* discussion *infra* Part I(B).

43. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y.

44. The Department of Justice Criminal Resource Manual is a supplement to the Justice Manual, a collection of publicly available DOJ policies and procedures used to provide internal guidance to the Department. There are nine titles in the Justice Manual, each with its own corresponding Resource Manual. Title 9 of the Justice Manual covers the Criminal Division of the DOJ, and the Criminal Resource Manual contains supplementary materials.

45. U.S. DEP'T OF JUSTICE, CRIMINAL RESOURCE MANUAL, § 279(B), https://perma.cc/TZ5J-U2JC.

subpoenas.[46] In determining whether to authorize such a subpoena, the OIA considers the indispensability of the records to the investigation and the availability of alternative methods such as MLATs and letters rogatory.[47]

4. Implications of the Carpenter Decision and the Warrant-Subpoena Distinction

Along with the subpoenas just discussed, U.S. prosecutors also commonly use a different instrument, the warrant. The similarities and differences between subpoenas and warrants has become a topic that, as discussed further below, may affect judicial interpretation of the CLOUD Act. A warrant gives law enforcement officers special privileges to search or seize an individual or location under the authority of the court. To obtain a warrant, the Fourth Amendment requires that law enforcement prove to the court that it has probable cause that the search will find evidence of the crime being investigated. This requirement was influenced in part by English common law in *Entick v. Carrington,*[48] a prominent decision from 1765 that the U.S. Supreme Court has cited in developing Fourth Amendment jurisprudence. The case involved actions against state officers who raided people's homes and other places in search of materials connected with pamphlets attacking government policies and the King. The court found that the officers were trespassing on the claimant's land and that an individual could prevent access to his property unless that access was granted by law. The officers had claimed they were acting pursuant to general warrants. The court held that issuance of a warrant for seizure of "all" papers as opposed to only those allegedly criminal in nature was not authorized by law. This shaped the limits on governmental power to search and seize documents.

---

46. *Id.* ("The request must be in writing and set forth:

(1) The subject matter and nature of the grand jury investigation or trial;
(2) A description of the records sought including their location and identifying information such as bank account numbers;
(3) The purpose for which the records are sought and their importance to the investigation or prosecution;
(4) The extent of the possibility that the records might be destroyed if the person or entity maintaining them becomes aware that they are being sought; and
(4) Any other information relevant to OIA's determination.").

47. *Id.* ("The following considerations will be taken into account in determining whether such a subpoena should be authorized:

(1) The availability of alternative methods for obtaining the records in a timely manner, such as use of mutual assistance treaties, tax treaties or letters rogatory;
(2) The indispensability of the records to the success of the investigation or prosecution; and
(3) The need to protect against the destruction of records located abroad and to protect the United States' ability to prosecute for contempt or obstruction of justice for such destruction.").

48. *See* Entick v. Carrington (1765) Eng. Rep. 807 (K.B.).

A subpoena, in contrast to a warrant, is an instrument that directs an individual or entity to produce certain objects or information. A common type of subpoena relevant to law enforcement purposes is the grand jury subpoena. Grand juries can serve individuals or corporations with subpoenas for production of documents that could aid in deciding whether to indict an individual for a criminal offence. These subpoenas are served in accordance with Federal Rules of Criminal Procedure.[49] Under Rule 17, a subpoena can order the recipient to produce any books, papers, documents, data, or other objects the subpoena designates. The subpoena may direct a person or entity to produce the items in court before trial or before they are to be offered in evidence.

Unlike with warrants, a grand jury does not need to show probable cause to call witnesses or subpoena documents. Instead, the grand jury can issue a subpoena if the documents might reasonably be relevant to the investigation. In response, the recipient can move to quash or modify a subpoena if compliance would be "unreasonable or oppressive."[50] Since a subpoena involves "the compulsory production of private papers," the recipient is entitled to the Fourth Amendment protection against unreasonableness.[51] A common test for reasonableness asks whether "the materials requested are relevant to the investigation, whether the subpoena specifies the materials to be produced with reasonable particularity, and whether the subpoena commands production of materials covering only a reasonable period of time."[52]

In *Carpenter v. U.S.*, the Supreme Court held that a probable cause warrant was required for obtaining cell-site location information from a third party.[53] Some commentators have argued that this might mean an important change in the law of subpoenas and application of the Fourth Amendment. Before *Carpenter*, the Fourth Amendment has had limited application to subpoenas – subpoenas could be challenged only on the ground that they were unduly burdensome or oppressive. The Court's majority opinion suggests that this limited application of the Fourth Amendment to subpoenas is because of the third party doctrine – a

49. FED. R. CRIM. P. 17 ("A subpoena must state the court's name and the title of the proceeding, include the seal of the court, and command the witness to attend and testify at the time and place the subpoena specifies. The clerk must issue a blank subpoena—signed and sealed—to the party requesting it, and that party must fill in the blanks before the subpoena is served.").

50. FED. R. CRIM. P. 17(c)(2).

51. *See* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J. L. & TECH. 543, 546 (2011), https://perma.cc/26U9-8RH3 ("Unlike the issuance of a warrant, however, which allows law enforcement to search and seize property immediately, the issuance of a subpoena 'commences an adversary process during which the person served with the subpoena may challenge it in court before complying with its demands.' The additional level of constitutional protection afforded by the probable cause standard for warrants is not necessary for subpoenas because the judicial process that precedes production should ensure that the constitutional reasonableness standard is met," citing United States v. Bailey *(In re* Subpoena Duces Tecum*)*, 228 F.3d 341, 348 (4th Cir. 2000)).

52. *Id.* at 547 (citing *In re* Grand Jury Matters, 751 F.2d 13, 18 (1st Cir. 1984); *see, e.g.*, United States v. Alewelt, 532 F.2d 1165, 1168 (7th Cir. 1976); United States v. Gurule, 437 F.2d 239, 241 (10th Cir. 1970)).

53. *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

suspect generally does not have legitimate privacy interest in records held by a third party. In *Carpenter*, the Court limited the scope of the third party doctrine and held that a probable cause warrant is required for the government to access cell-site location information held by third parties, such as telephone companies.

In his dissent, Justice Alito argued against what he found to be a wrongful conflation of warrants and subpoenas. Justice Alito argued that the majority opinion wrongly found that a Fourth Amendment "search" of Carpenter occurred and therefore applied requirements for actual searches and seizures to a subpoena issued to a third-party service provider. Justice Alito also argued that this construction wrongly extends greater protections to third-parties related to a subpoena than to the target of the subpoena itself. Justice Alito writes

> . . .[E]ven if the Fourth Amendment permitted someone to object to the subpoena of a third party's records, the Court cannot explain why that individual should be entitled to greater Fourth Amendment protection than the party actually being subpoenaed. When parties are subpoenaed to turn over their records, after all, they will at most receive the protection afforded by [the subpoena cases] even though they will own and have a reasonable expectation of privacy in the records at issue. Under the Court's decision, however, the Fourth Amendment will extend greater protections to someone else who is not being subpoenaed and does not own the records. That outcome makes no sense, and the Court does not even attempt to defend it.[54]

In response to Justice Alito's concerns, the majority opinion concedes Justice Alito's historical accounting of the distinctions between subpoenas and warrants, but suggests that the history is inapposite as "[t]his Court has never held that the Government may subpoena third parties for records *in which the suspect has a reasonable expectation of privacy*."

Indeed, some scholars have argued that the majority decision restores an equilibrium that was previously unbalanced by the rise of remote data storage. Professor Orin Kerr wrote that "in the world of local storage," law enforcement must engage in a physical search to obtain data held by a target and therefore must abide by the Fourth Amendment and its warrant requirement in doing so. The target may also invoke their Fifth Amendment privilege against self-incrimination if compelled to provide such information by a subpoena. With remote storage, however, that information is held by a separate corporate entity, often located far away, and which has no Fifth Amendment rights to assert on behalf of its users. Kerr argues that "[a]pplying the usual subpoena standard when the target has Fourth Amendment rights would result in a dramatic expansion of government power that would let the government get everything with few limits." Instead, Kerr argues, the Court in *Carpenter* restored equilibrium by treating

54. *Id*. at 2256 (Alito, J., dissenting).

remote storage in the same way as if the data had been stored locally by the user.[55]

B. The Microsoft Ireland Case and Ability of U.S. Law Enforcement to Access Electronic Communication Stored Overseas

In this section, we discuss the district court and the Second Circuit decisions in *Microsoft Ireland* and key arguments made by the DOJ and Microsoft. The discussion helps to understand the different views about U.S. law enforcement's powers to compel production of communications content stored outside the U.S.

Microsoft Ireland involved the DOJ seeking evidence from a company in a criminal investigation about a customer of that company. The request for customer records was in that respect similar to that in Bank of Nova Scotia, where the bank held the records and the investigation involved its customers. In this case, a warrant was issued in December 2013 to Microsoft-U.S. for emails of a suspect in a narcotics investigation. The warrant was issued pursuant to Section 2703(a) of the Stored Communications Act (SCA), the U.S. law that governs law enforcement access to stored electronic communication.[56] Section 2703(a) allows law enforcement to require disclosure of communication in storage for 180 days or less through a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.[57] The SCA contained no provision specifically addressing whether the government could obtain customer data held outside the U.S. In response to the warrant, Microsoft produced emails that were held on servers within the U.S. but refused to produce emails on its server in Ireland. Microsoft sought to quash the warrant, arguing that the SCA did not envisage production of stored communications content beyond U.S. boundaries and that the government would have to pursue other bilateral channels for such information, such as an MLAT request. A federal magistrate denied Microsoft's plea.

The Southern District of New York affirmed the magistrate's order and held that Microsoft must comply with the warrant.[58] In doing so, the federal district court noted the U.S. government's ability to enforce subpoenas for records stored outside the U.S. following the Bank of Nova Scotia doctrine.[59] The District Court characterized an SCA warrant as a hybrid between a traditional warrant and a

55. Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, LAWFARE BLOG (June 26, 2018, 6:44 PM), https://perma.cc/G7R5-9PTH.

56. The Stored Communication Act was enacted as Title II of the Electronic Communications Privacy Act (ECPA). The ECPA was passed in 1986 to extend government restrictions on wiretaps to electronic communications. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

57. 18 U.S.C. § 2703(a) (2010). Rule 41 of the Federal Rules of Criminal Procedure describes the process of issuing a warrant. A search warrant can be issued by a magistrate judge on application by a law enforcement officer or an attorney for the government, upon a showing of probable cause of a crime. FED. R. CRIM. P. 41.

58. *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (order reflecting ruling made at oral argument; stayed pending appeal).

59. *Id.*; *see* Eleni Kyriakides, *Federal District Court Rules that Warrants Cover Email Content Stored Abroad*, CTR. FOR DEMOCRACY & TECH. BLOG (Aug. 1, 2014), https://perma.cc/SP9Y-NUDB.

subpoena—unlike a traditional warrant, an SCA warrant was executed by a service provider rather than a government law enforcement agent and its execution did not require the presence of an agent.[60] In that sense, the district court held that SCA warrants were closer to subpoenas and could require the recipient to produce information in its "possession, custody or control" regardless of the location of that information.[61]

Microsoft appealed the district court's order to the Second Circuit. The Second Circuit ruled for Microsoft based largely on a canon of statutory interpretation.

1. Microsoft's Position: The SCA did not Authorize Warrants to Operate Beyond the U.S.

Microsoft argued that the SCA did not authorize warrants for seizure of customer emails in other countries, and that the case involved a warrant for a search that would take place outside of the country.[62] Microsoft cited a canon of statutory interpretation, that there is a presumption against extraterritorial application of a law,[63] and argued that the presumption should bar the SCA's application to content stored overseas. In Microsoft's view, Congress had given no indication that warrant provisions in the Electronic Communications Privacy Act (ECPA) would apply extraterritorially, and such a warrant was an unauthorized extraterritorial application of Section 2703(a) since it compelled Microsoft to conduct a

60. *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 15 F. Supp. 3d 466 (S.D.N.Y. 2014). A warrant is issued by a magistrate judge and authorizes law enforcement officers to conduct "searches". A subpoena directs the recipient to produce the described evidence. A law enforcement officer need not be physically present at the site of a search in case of a subpoena; instead, subpoena recipients are required to gather the evidence themselves and produce it. For the distinction between warrants and subpoenas in light of the Supreme Court decision in Carpenter see Kerr, *supra* note 55.

61. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (2017), *and vacated and remanded sub nom.* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

62. Brief for Appellant at 19, *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv).

63. Microsoft, 829 F.3d at 210 ("When interpreting the laws of the United States, we presume that legislation of Congress 'is meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears. Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010) . . . This presumption rests on the perception that 'Congress ordinarily legislates with respect to domestic, not foreign matters.' Id. The presumption reflects that Congress, rather than the courts, has the 'facilities necessary' to make policy decisions in the 'delicate field of international relations.' . . . In line with this recognition, the presumption is applied to protect against 'unintended clashes between our laws and those of other nations which could result in international discord.' Equal Emp't Opportunity Comm'n v. Arabian American Oil Co., 499 U.S. 244 (1991).

To decide whether the presumption limits the reach of a statutory provision in a particular case, 'we look to see whether "language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control."' Aramco, 499 U.S. at 248, 111 S.Ct. 1227 (alteration in original) (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285, 69 S.Ct. 575, 93 L.Ed. 680 (1949)). The statutory provision must contain a 'clear indication of an extraterritorial application'; otherwise, 'it has none.' Morrison, 561 U.S. at 255, 130 S.Ct. 2869; *see also* RJR Nabisco, 579 U.S. at ——, 136 S.Ct. 2090.").

law enforcement search and seizure in Ireland.[64]

Microsoft also argued that the district court erred in classifying the warrant as a hybrid subpoena and that there was no basis in the statute's text for this conclusion. Congress's use of "warrant" in the SCA was a choice to refer to a particular legal process and should be respected. Microsoft also distinguished *Marc Rich*[65] because that case applied to subpoenas for a company's own business records. In Microsoft's view, the Marc Rich approach could not be applied to require a "caretaker to import a customer's private papers and effects from abroad."[66]

2. The Government's Position: An SCA Warrant is Like a Subpoena and the Test for Production is Control not Location

The government characterized the dispute as a question of compelled disclosure arguing that the label of the instrument did not matter.[67] Under such characterization, an SCA warrant operated like a subpoena and would require the recipient to deliver records regardless of location, as long as the records were within the recipient's custody or control (following *Marc Rich*). On extraterritoriality, the government argued that nothing in the SCA's text or legislative history indicated that compelled production of records was limited to records stored domestically.[68] The statute only placed a requirement on a service provider to disclose customers' data, with no reference to any territorial restriction. Also, in the government's view, since the test for production of documents was control and not location, the disclosure was actually taking place within the United States and was, therefore, not extraterritorial.

3. The Second Circuit Held That an SCA Warrant Was Different From a Subpoena

The Second Circuit held that warrants and subpoenas were distinct legal instruments.[69] In the court's view, Section 2703 of the SCA recognized this distinction and used the term "warrant" to "signal a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level" of protection.[70] The SCA gave no indication that it was intended to operate

64. Brief for Appellant, *supra* note 62, at 20, 26.

65. *See* discussion *supra* Part I(A).

66. Brief for Appellant, *supra* note 62, at 16 ("The Marc Rich rule stems from a presumption that companies have control over their own books. That rule has never been applied to require a caretaker to import a customer's private papers and effects from abroad. Thus, a bank can be compelled to produce the transaction records from a foreign branch, but not the contents of a customer's safe deposit box kept there. A customer's emails are similarly private and secure and not subject to importation by subpoena.").

67. Microsoft, 829 F.3d at 201.

68. Brief for the United States at 26, *In re* A Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

69. *See* Microsoft, 829 F.3d at 214 (citing Black's Law Dictionary).

70. Under the Stored Communications Act, law enforcement can require disclosure of contents that are in storage for 180 days or less through a warrant. For content that has been in storage for more than 180 days, law enforcement can require disclosure through (a) a warrant; (b) through an administrative or

extraterritorially and the use of the term of art "warrant" emphasized the domestic boundaries of the law.[71] The court held that the *Marc Rich* test was developed in the context of subpoenas and in the absence of any firm indication in the law, could not be imported into the law relating to judicially issued warrants. In addition, the court took note of the *Bank of Nova Scotia* line of cases relied on by the district court but distinguished those from the present dispute, observing that bank depositors had no protectable privacy rights in a bank's records regarding their accounts.[72]

The Second Circuit's ruling turned on the interpretation of the instrument and the statute—that Section 2703(a) expressly called the legal instrument a "warrant". The court reasoned that the history associated with the use of warrants, rather than subpoenas, should thus apply. While the Second Circuit did not expressly rule on the meaning of "control," it did note that Microsoft was different from the defendant in *Marc Rich*, who was asked to produce records in which only the defendant corporation, rather than a customer, had a protectable privacy interest.[73]

There were also calls for a more nuanced approach that could only be addressed by Congress. One of the judges on the Second Circuit panel, Judge Lynch,[74] in his concurring opinion, expressed skepticism towards the notion that the location of a server chosen by a service provider should be controlling, "putting those communications beyond the reach of a purely 'domestic' statute."[75] At the same time, enabling a government to demand communications, without

---

a grand jury or trial subpoena; or (c) through a court order. However, in United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010), the Sixth Circuit held that the Fourth Amendment prevents law enforcement from obtaining stored e-mail communications without a warrant based on probable cause; *see also* United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) ("'[I]ndividuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.'" (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011))). After *Warshak*, the Department of Justice updated its practice when seizing stored electronic communications to require law enforcement to require for its own prosecutions a judge-issued warrant in compliance with the protections of the Fourth Amendment to the US Constitution. *ECPA (Part 1): Lawful Access to Stored Content: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec. and Investigations of the H. Comm. on the Judiciary*, 113th Cong. 14 (2013) (statement of Elana Tyrangiel, Acting Assistant Att'y Gen., Office of Legal Policy, Department of Justice).

71. A warrant's reach is limited geographically. *See* FED. R. CRIM. P. 41(b)(5).

72. United States v. Miller, 425 U.S. 435 (1976). In *Miller*, the Supreme Court found that bank records were not subject to Fourth Amendment protection, stating that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers." The Supreme Court holding in *Miller* contrasts with later holdings of a protected privacy interest in the contents of emails in *Warshak* and in the location records at issue in *Carpenter*.

73. Microsoft, 829 F.3d at at 220-21.

74. *Id*. at 224. (Lynch, J., concurring).

75. *Id*. at 222 ("I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely 'domestic' statute. That may be the default position to which a court must revert in the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it

regard to other factors, also did not appear to strike the right balance. Judge Lynch urged Congress to step in to modernize the law to address the issue. Before the Supreme Court oral argument took place, Microsoft also issued a statement calling upon Congress to enact a statute balancing all competing concerns.[76]

4. European Perspective on the Microsoft Ireland Case

The *Microsoft Ireland* case attracted attention from multiple perspectives, including privacy scholars, companies in Europe, and the European Commission. Amici briefs were filed with the Supreme Court by Privacy International,[77] Digital Rights Ireland,[78] and EU Data Protection and Privacy Scholars,[79] among others. These generally supported Microsoft's arguments, following the Second Circuit approach against what they said was the extraterritorial application of the SCA and classification of an SCA warrant as a warrant. Many of these appeared to suggest that the decision to allow an SCA warrant to run beyond U.S. territories should be a matter for Congress.

The European Commission also filed a brief, not in support of either party, highlighting EU domestic law on the subject. Without taking a position on the construction of the SCA under U.S. law, the Commission submitted that it would be appropriate for the Supreme Court to consider EU domestic law on searches of data stored in the EU. In the Commission's view, such cases engaged the principles of territoriality and comity since a public authority was requiring a company established in its jurisdiction to produce data stored in a different jurisdiction.[80] The Commission submitted that the EU General Data Protection Regulation (GDPR) addressed the production of data stored in the EU and described the GDPR provisions for transfer of personal data to non-EU states. The relevant provision—Article 48—states that orders by courts in third countries, like the U.S., could only be recognized or enforceable "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."[81] In the Commission's view, the

---

can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness.").

76. Brad Smith, *A Problem Congress Should Solve*, MICROSOFT ON THE ISSUES (Feb. 27, 2018), https://perma.cc/6BFR-5Q72.

77. Brief of Privacy International et al. as Amici Curiae in Support of Respondent, United States v. Microsoft Corp., 138 S.Ct. 1186 (2018) (No. 17-2).

78. Brief of Amici Curiae Digital Rights Ireland Ltd. & the Open Rights Group in Support of Microsoft Corp., United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

79. Brief of EU Data Protection & Privacy Scholars as Amici Curiae in support of Microsoft, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

80. Brief of the European Commission on Behalf of the European Union as Amici Curiae in Support of Neither Party at 6, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

81. Council Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 48, 2016 O.J. (L 119) 1 [hereinafter GDPR]. One of the authors of the current paper, Swire, is now writing separately about the extent to which, and under what circumstances, Article 48 of the General Data

GDPR thus made MLATs the preferred option for transfers. However, the Commission pointed out two other lawful grounds for transfer:[82] transfers necessary for "important reasons of public interest";[83] and transfers necessary for purposes of "compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject."[84]

5. Supreme Court Oral Argument and Implications for Meaning of "Control"

The Supreme Court oral argument in February 2018 focused on two issues: whether an SCA warrant was a warrant, a subpoena, or a hybrid as suggested by the district court; and whether there was any extraterritorial conduct involved in Microsoft producing the documents.[85] Before the Supreme Court, the government reiterated its stance and argued that the case involved a domestic application of Section 2703—the conduct relevant to Section 2703's focus was disclosure of records and such disclosure would occur in the U.S.[86] Microsoft could comply with the warrant by undertaking acts entirely within the U.S. In the government's view, Congress enacted the SCA in 1986 against a backdrop of settled law and longstanding principles relating to subpoenas—that the recipient produces documents within its control, even if it chooses to store those materials abroad.[87]

The Court also questioned Microsoft and the DOJ on whether Congress might be better suited to resolve the issue.[88] At the time, Congress was considering the

---

Protection Regulation acts as a blocking statute, to prevent transfers of personal data to third countries such as the U.S.

82. *Id*. art. 49. The Commission pointed out that Article 49 was titled "Derogations for specific situations" and would be interpreted strictly.

83. Brief for the European Commission on Behalf of the European Union as Amici Curiae Supporting Neither Party, *supra* note 80, at 15 ("[T]o qualify, this 'public interest' must be one 'recognised in Union law or in the law of the Member State to which the controller is subject.' *Id*. art. 49 (4). In general, Union as well as Member State law recognize the importance of the fight against serious crime—and thus criminal law enforcement and international cooperation in that respect—as an objective of general interest. Case C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, ¶ 42, ECLI:EU:C:2014:238; Opinion 1/15, ¶ 148, ECLI:EU:C:2017:592.").

84. Brief for the European Commission on Behalf of the European Union as Amici Curiae Supporting Neither Party, *supra* note 80, at 10 ("The legitimate interest could, again, be the interest of the controller in not being subject to legal action in a non-EU state. Such transfers are permissible 'only if the transfer is not repetitive,' only if it 'concerns only a limited number of data subjects,' and only if 'the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.' Relevant circumstances might include procedural guarantees under which the foreign court order was adopted, as well as applicable data protection rules in place in the third country. The controller must also 'inform the supervisory authority of the transfer.'").

85. *See* Andrew Keane Woods, *Recap: Oral Arguments in Microsoft-Ireland*, LAWFARE BLOG (Feb. 27, 2018, 2:35 PM), https://perma.cc/6T7T-PM3P.

86. Brief for the United States at 17, United States v. Microsoft Corp., 138 S.Ct. 1186 (No. 17-2).

87. *Id*. at 32.

88. Transcript of Oral Argument at 6, Microsoft Corp., 138 S.Ct. 1186 (No. 17-2) (Justice Ginsburg stating,"If Congress takes a look at this, realizing that much time and – and innovation has occurred since 1986, it can write a statute that takes account of various interests. And it isn't just all or nothing. So wouldn't it be wiser just to say let's leave things as they are; if – if Congress wants to regulate in this brave new world, it should do it?"); *Id*. at 12 (Justice Sotomayer stating, "Now I understand there's a bill that's being proposed by bipartisan senators that would give you most of what you want but with great

bill that became the CLOUD Act; Congress eventually enacted it into law in April 2018. Following the law's passage, the Supreme Court declared the *Microsoft Ireland* case moot and did not rule on the territorial reach of U.S. law.

Questions have since been raised as to whether the CLOUD Act expanded the scope of DOJ's power. The answer to this depends on one's assessment of prior practice and whether DOJ or Microsoft was likely to prevail in the *Microsoft Ireland* case.[89] If one believed that Microsoft would have prevailed, then the storage of the emails in Ireland would have been outside the power of DOJ to access under the SCA. On that view, the CLOUD Act expanded DOJ's access. On the other hand, if one believed that DOJ would have prevailed, then the CLOUD Act did not expand DOJ authority – the new law reiterated the possession, custody, or control test that already applied. Along with other authors,[90] one of the authors (Swire) has written previously that DOJ was likely to prevail in the Supreme Court.[91]

C. Passage of the CLOUD Act Codified the "Possession, Custody or Control" Test

Before the Supreme Court could rule on *Microsoft Ireland*, the U.S. Congress passed the CLOUD Act.[92] The CLOUD Act has two key parts. One part responds to foreign governments' concerns about U.S. laws that restrict foreign law enforcement's access to communications content held by U.S. service providers—restrictions that apply even when foreign governments are seeking to access data regarding their own nationals in the investigation of local crime. This part of the CLOUD Act authorizes the creation of executive agreements that would lift those restrictions and enable foreign governments to access communications content directly from U.S.-based service providers, subject to a set of privacy protections and other conditions.

The other part, relevant to our discussion, clarifies the rules governing U.S. law enforcement access to data in the hands of U.S. service providers. This part was enacted in response to the Second Circuit decision in *Microsoft Ireland* that warrants issued under the Stored Communication Act only reached data held within the territorial borders of the United States. As a result of this ruling, while the case was pending appeal to the U.S. Supreme Court, U.S.-issued warrants could not, at least within the Second Circuit, compel U.S. providers to disclose

protections against foreign conflicts. There are limitations involving records that are stored abroad. Why shouldn't we leave the status quo as it is and let Congress pass a bill in this new age. . ."). *See also* Woods, *supra* note 85.

89. The discussion in the text follows discussion in Peter Swire & Jennifer Daskal, *Frequently Asked Questions about the U.S. CLOUD Act*, CROSS-BORDER DATA FORUM (Apr. 16, 2019), https://perma.cc/V2KY-NAMK.

90. *See* Jennifer Daskal, *Unpacking the CLOUD Act*, 4 EUCRIM 220, 220-225 (2018), https://perma.cc/HF82-L7QW; Eric Wenger, *Does the Cloud Act Really Grand DOJ Sweeping New Powers?*, CROSS-BORDER DATA FORUM (Aug. 27, 2018), https://www.crossborderdataforum.org/does-the-cloud-act-really-grant-doj-sweeping-new-powers/.

91. *See* Swire & Daskal, *supra* note 89.

92. *See id.*; Peter Swire & Jennifer Daskal, *What the CLOUD Act Means for Privacy Pros*, IAPP (Mar. 26, 2018), https://perma.cc/E47E-PTCK.

communications content stored outside of the U.S. even if that data were accessible from within the U.S.[93] At least five federal courts outside the Second Circuit had reached the contrary result—that warrant authority under the SCA reached communications within a service provider's possession, custody, or control regardless of the location of the servers.[94] Simply as a matter of describing then-applicable U.S. law, a clear majority of the federal courts that addressed the matter agreed with the DOJ position.

The CLOUD Act mooted the pending *Microsoft Ireland* Supreme Court decision. It stated clearly the importance of the possession, custody, or control test. The Act amended the SCA to read:

> 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.[95]

In other words, the SCA's warrant authority now requires companies to produce data in their "possession, custody, or control," subject to the new statutory language "regardless of the physical location where the data may be stored." Part II of this Article analyzes the possession, custody, or control test.

The Act also provided two comity provisions. One creates a new statutory basis for providers to move to quash in limited situations where there is a conflict with the law of a "qualifying foreign government" (i.e., a government that has entered into an executive agreement under the CLOUD Act). The other explicitly preserves the availability of common law comity claims in situations where the new statutory-based claims are unavailable.[96] Both the U.S. government and the tech companies supported these changes.[97]

---

93. *See* Marshall Cohen, *Prosecutors Used a New Law Trump Signed to Get Data from Cohen's Gmail*, CNN POLITICS (Mar. 19, 2019, 11:06 AM), https://www.cnn.com/politics/live-news/michael-cohen-search-warrant-documents-dle/index.html (reporting that the FBI was unable to obtain data from Cohen's Gmail account stored on servers outside the U.S. in February 2018, but were able to get a new search warrant approved in April 2018 after the Cloud Act was in force).

94. *See, e.g.*, In re Info. Associated with @gmail.com, No. 16–mj–00757, 2017 U.S. Dist. LEXIS 130153, 2017 WL 3445634, at *36 (D.D.C. July 31, 2017) ("[T]he SCA warrant [is] simply a domestic execution of the court's statutorily authorized enforcement jurisdiction over a service provider, which may be compelled to retrieve electronic information targeted by the warrant, regardless of where the information is 'located'. . ."); *In re* Search Warrant No. 16-960-M-01 to Google, 275 F. Supp. 3d 605, 606 (E.D. Pa. 2017); *In re* Search of Information Associated with Accounts Identified as [Redacted] @gmail.com, 268 F. Supp. 3d 1060, 1071 (C.D. Cal. 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *4 (N.D. Cal. Apr. 25, 2017).

95. 18 U.S.C. § 2713 (2012).

96. *See* 18 U.S.C. § 2713(b)-(c).

97. Swire and Daskal, *supra* note 92.

II. THE HISTORY OF "POSSESSION, CUSTODY, OR CONTROL" IN U.S. LAW

Since the CLOUD Act lacks a statutory definition of "possession, custody, or control," courts will likely look to other uses of this term of art in U.S. law when interpreting the meaning of this phrase. The same language of "possession, custody, or control" is central to the rules governing the scope of subpoenas and discovery in the Federal Rules of Civil and Criminal Procedure, and thus has been litigated in those contexts. This section will first look at the how this phrase is used in the contexts of the CLOUD Act and the Federal Rules. Next, it will examine a series of situations in which courts have found or would be likely to find that an entity has "control" over data based on an assessment of legal and practical or day-to-day control of the data. Finally, it will examine four themes related to control under the CLOUD Act.

First, it is important to examine how the phrase operates in the context of the CLOUD Act. The CLOUD Act amended the Stored Communications Act to include a new section that reads:

> 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."[98]

Here, the phrase "possession, custody, or control" acts as a bound on the scope of information that a service provider can be required to preserve, backup, or disclose under the Act. The exact same phrase appears in a similar context in the Federal Rules of Civil and Criminal Procedure ("the Rules") as a bound on the scope of documents parties and non-parties to litigation can be required to disclose:

1. Federal Rules of Civil Procedure Rule 34(1)(A): "A party may serve on any other party a request . . . to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's **possession, custody, or control**. . ." including "any designated documents or electronically stored information . . . stored in any medium."
2. Federal Rules of Civil Procedure Rule 45(1)(A): "Every subpoena must . . . command each person to whom it is directed to do the following at a specified time and place: attend and testify; produce designated documents, electronically stored information, or tangible things in that person's **possession, custody, or control**. . ."

98. 18 U.S.C. § 2713 (emphasis added).

3. Federal Rules of Criminal Procedure Rule 16(a)(1)(B, D-F): "Upon a defendant's request, the government must provide or provide access to the defendant's written or recorded statements, the defendant's prior criminal record, any documents or objects, and any results or reports of any physical or mental examination and any scientific test or experiment if the information is within the government's **possession, custody, or control**."

Like the CLOUD Act, the Rules offer no further definition of this phrase. Unlike the CLOUD Act, however, the Rules have been thoroughly litigated in the past, resulting in a body of jurisprudence examining how to determine when and how an entity can control data.

A. Interpreting "Possession, Custody, or Control" Under the Federal Rules of Civil and Criminal Procedure

This section will walk through a series of four contexts where a court might find an entity has "control" over electronic evidence.[99] Courts have varied in their means of analyzing control, with some looking to whether there is a "legal right" to the data and some examining whether an entity has the "practical ability" to access the data.[100] This section will posit that these differing inquiries make sense when taken in the framework described in Figure 1,[101] where judges will look along two potential dimensions of dispute: whether the entity has legal control over the data, and/or whether the entity has day-to-day—or *de facto*—control over the data. This section will show how, based on the factual circumstances of a particular case, the courts have examined either or both of those axes of dispute in interpreting the Rules.

As a preliminary point, the history of the Rules themselves suggests that courts will seek to harmonize interpretations of this phrase in different contexts, when possible. In *United States v. Stein*, the U.S. District Court for the Southern District of New York wrote of the phrase's appearance in both the Criminal and Civil Rules that "[c]ommon sense, not to mention settled principles of

99. The definitions of "possession" and "custody" have rarely been litigated, as they both refer to a binary "yes or no" proposition: either the targeted entity has possession or custody of the evidence sought, or not, whereas establish "control" is less clear. *See, e.g.*, S. Peninsula Hosp. v. Xerox State Healthcare, LLC, No. 3:15-CV-000177-TMB, 2019 WL 1873297, at *5 (D. Alaska Feb. 5, 2019) (finding that the defendant's provision of database services to the state of Alaska meant the defendant had possession and custody of the database in question and could be required to produce that information).

100. *See generally* 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 (2016) (analyzing inconsistencies among interpretation of the Rules of Civil Procedure in different districts and grouping those decisions into camps based on whether the decisions hinge on establishing if the target has a "legal right" to the evidence, or if the target has the "practical ability" to access the evidence).

101. *See supra* Figure 1.

construction, suggests a uniform construction [between the two]."[102] By the same logic, the term's appearance in the CLOUD Act would warrant applying the same uniform construction, including drawing on existing jurisprudence examining the phrase's operation in the rules.

1. U.S.-Based Corporation

In this first example, consider a corporation with its headquarters in Delaware in the U.S. and a foreign branch in the U.K. The branch has a local manager but is under the direction of corporate headquarters, and the company's CEO and his management team oversee operations in both locations. In this instance, if the Department of Justice were to issue a subpoena to the company to turn over data held by the U.K. branch, the company would almost certainly be found to have control over that data.[103] Indeed, as explained earlier, this scenario falls squarely within the *Bank of Nova Scotia* doctrine where a corporation can be compelled to turn over data held by foreign branches.[104] Nor did our research discover any cases where these facts would not be found to establish control over the branch's data. In short, this scenario would likely fall at the highest end of the "legal control" axis, as depicted below, as there is both clear legal control (as explained under the *Bank of Nova Scotia* doctrine) as well as day-to-day control (since the branch operates in conjunction with the home office).

2. Subsidiaries

A company can also be found to have control over a related company where it holds a sufficiently controlling ownership interest. In this second example, consider that the U.K. office is not a branch of the company, but rather a wholly-owned subsidiary. In this instance, the U.S. parent company may be a separate legal entity, but would still almost certainly be found to have control over the U.K. subsidiary's data.[105] With full control over its subsidiary, the parent company would have the legal ability to direct the use or transfer of the subsidiary's data, demonstrating legal control over the data.

Nor is 100% ownership the only scenario where the U.S. entity could have control over the related entity. In this case, it is helpful to look at similar ways of establishing control in the banking sector. The Bank Holding Company Act defines a "bank holding company" as "any company which has **control** over

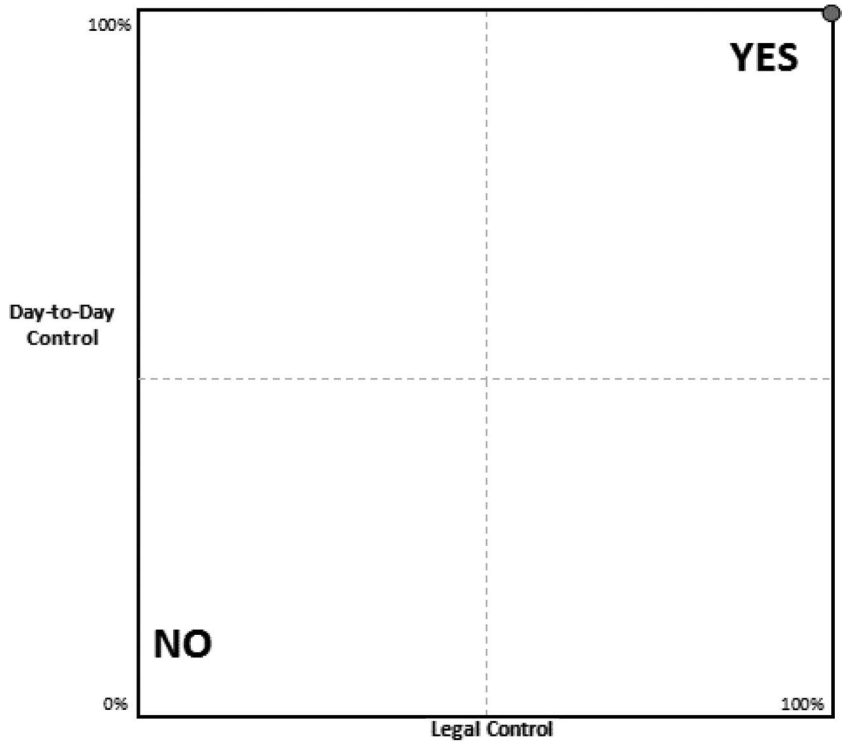
102. United States v. Stein, 488 F. Supp. 2d 350, 361 (S.D.N.Y. 2007).

103. While there may still be reasons why the entity would be able to avoid producing the data—such as seeking to have the subpoena quashed for principles of comity or being overly burdensome—in this section we will focus solely on the likelihood of establishing "control" over the data.

104. *See supra* Part I(A)(1).

105. *See* Strom v. Am. Honda Motor Co., 667 N.E.2d 1137, 1144 (Mass. 1996) (defining control as when "the information sought is in the possession or custody of a wholly owning parent (or virtually wholly owning) or wholly owned (or virtually wholly owned) subsidiary corporation, or of a corporation affiliated through such a parent or subsidiary").

Figure 4:
Clear Legal Control



any bank or over any company that is or becomes a bank holding company by virtue of this chapter."[106] The statute defines "control" to include where "the company directly or indirectly or acting through one or more other persons owns, controls, or has power to vote **25 per centum** or more of any class of voting securities of the bank or company."[107] The statute also, however, presumes that a company that owns, controls, or has the power to vote less than **5** percent of any class of voting securities does **not** have control over the other entity.[108]

For this example, a court would almost certainly find that a parent has control over a wholly-owned subsidiary for purposes of the CLOUD Act. It would likely

106. 12 U.S.C. § 1841(a)(1) (2012) (emphasis added).

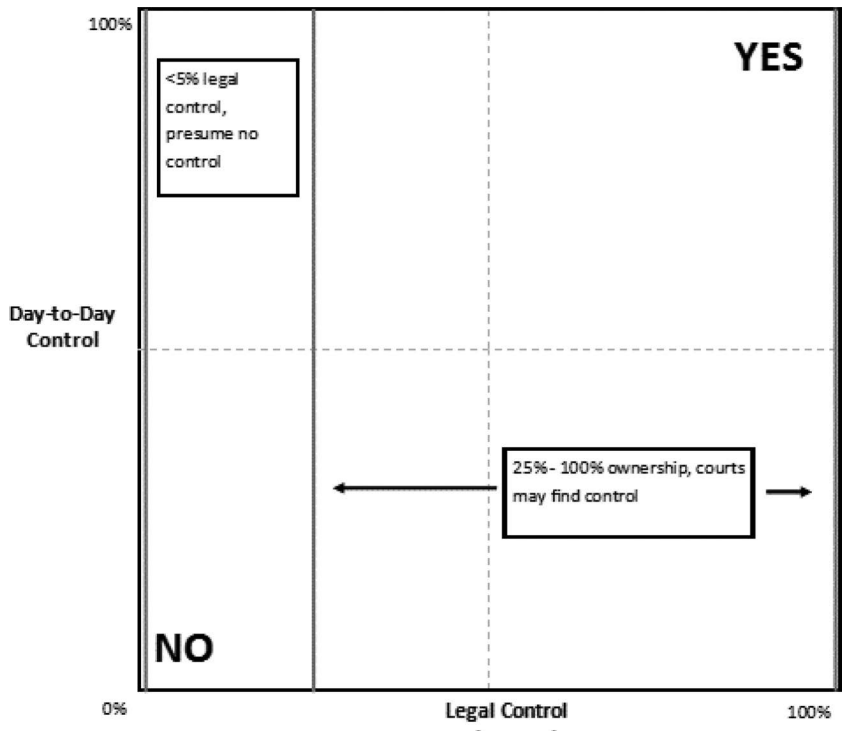
107. *Id.* § 1841(a)(2)(A) (emphasis added). The statute also defines control to include where "(B) the company controls in any manner the election of a majority of the directors or trustees of the bank or company; or (C) the Board [of Governors of the Federal Reserve System] determines, after notice and opportunity for hearing, that the company directly or indirectly exercises a controlling influence over the management or policies of the bank or company." *Id.*

108. *Id.* § 1841(a)(3).

also find control for less than 100 percent ownership. As a common-sense matter, majority ownership may be enough to establish legal control. With the Bank Holding Company Act as a guideline, one could imagine a court finding that anywhere from 25 – 100 percent ownership of an entity would be sufficient to establish control for purposes of the CLOUD Act. In at least some factual settings, however, a 25 percent level may be too low to establish control, notably if a majority owner opposed an action.

Conversely, a low enough level percentage of ownership could lead to the conclusion that there is not legal control. Courts could follow the Bank Holding Company Act's presumption that some level of *de minimis* ownership (e.g., less than 5 percent) demonstrates the company does not have control over the other entity. While these would likely not be firmly set lines, as other factual considerations could warrant a finding of control or no-control, it does provide a possible starting framework to consider where there is sufficient legal control by virtue of an ownership interest between the two entities to warrant finding control over the data.

Figure 5:
Legal Control Continuum



3. Co-Mingled Directors and Day-To-Day Control

In the absence of a controlling ownership, other indicia may also establish control. In this example, consider two legally unrelated companies that share the same board and CEO. In this case, a U.S. company would not have a legal ownership over a U.K. company, but an identical set of individuals would have control over both separate entities. In this case, courts have previously found that such co-mingling of leadership can be at least evidence to establish control for purposes of the Rules.[109] Similarly, the Bank Holding Company Act accounts for such a scenario by defining control to also include where the target company "controls in any manner the election of a majority of the directors or trustees of the bank or company."[110]

In this case, the courts are relying not only on legal ownership rights, but also on facts showing day-to-day control of operations. If the leadership in both companies is the same, then the U.S.-based company's management can have effective control over the activities of the U.K.-based company. Extending this idea further, the Bank Holding Company Act also defines control to include where its governing board "determines, after notice and opportunity for hearing, that the company directly or indirectly exercises a controlling influence over the management or policies of the bank or company."[111] For the CLOUD Act, one could see the presiding judge examining the role of the board in determining whether the facts demonstrate that the U.S.-based company can directly or indirectly control the management and policies of the U.K.-based company. Here again, the court would be seeking to determine whether there is a day-to-day control over the U.K.-based company, regardless of legal ownership or corporate relationships. In Figure 6 below, the horizontal lines show one possible continuum of day-to-day control where, regardless of the level of legal control, the judge might require the U.S. company to produce data held by the U.K. company.[112]

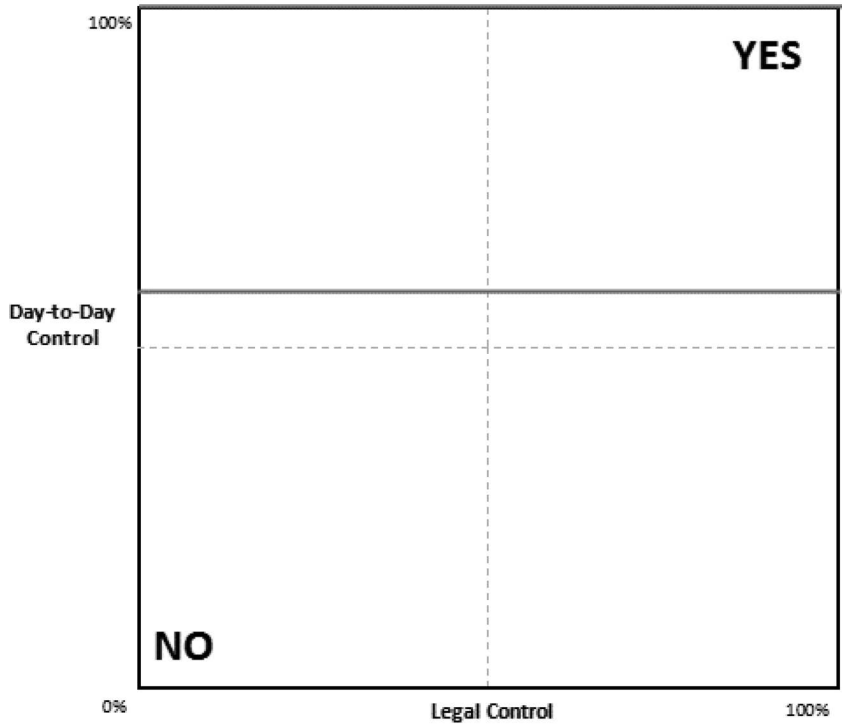
109. *See* Orthoarm, Inc. v. Forestadent USA, Inc., No. 4:06-CV-730-CAS, 2007 U.S. Dist. LEXIS 44429, at *7-8 (E.D. Mo. June 19, 2007) (ordering a U.S. subsidiary to produce documents held by the German parent company because both companies had "interlocking management structures" and had previously demonstrated "the ability to obtain documents from the parent company upon request"); *In re* Uranium Antitrust Litig., 480 F. Supp. 1138, 1152 (N.D. Ill. 1979) (determining that the U.S.-based subsidiary of a Canadian parent had control over documents held by the Canadian parent where evidence established that the two entities "operated as a single functional unit in all aspects of their uranium business" and "have shared an interlocking structure of corporate directors, officers, and executive and administrative personnel"). In these two cases, there was evidence both of legal control (the shared persons controlling the entities) and day-to-day control (proof of the ability to obtain documents upon request).

110. 12 U.S.C. § 1841(a)(2)(B) (2012).

111. *Id.* § 1841(a)(2)(C).

112. As with other uses of the diagram, we are not trying to establish the precise numeric percentage required to establish control. In this diagram, the horizontal line is slightly above a majority of day-to-day control. Consistent with our analysis, the horizontal line might be higher (e.g., roughly 90 percent of day-to-day control) or lower (e.g., anything over 50 percent control).

Figure 6:
Day-to-Day Control Continuum



4. Control in the Ordinary Course of Business

Day-to-day control can also include scenarios where data from the U.K. entity is handled by the U.S. entity in the ordinary course of business. Consider a relationship where the U.K. entity hires the U.S. entity as a human resources service provider. Under the ordinary course of business, the U.S. company would be regularly receiving, handling, and processing data that belongs to the U.K. entity. The activity need not occur literally every day, but if it is a routine business activity, then that type of relationship has established control for purposes of the Rules in previous cases.[113] Consequently, even though the U.S. entity would not have legal ownership or control over the data, and may in fact explicitly be a data processor,[114] the facts can support a finding of "control" for purposes of the CLOUD Act.

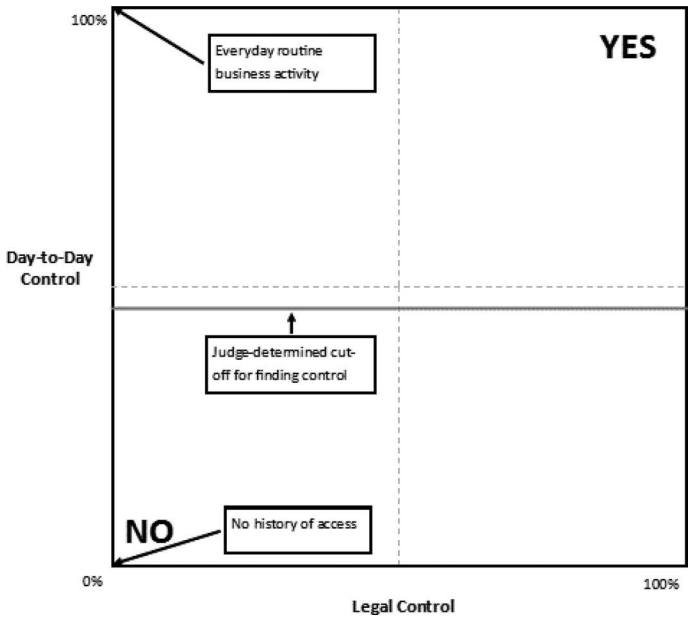
113. *See* First Nat'l City Bank of N.Y. v. Internal Revenue Serv., 271 F.2d 616, 618 (2d. Cir. 1959) (finding the bank had sufficient control over evidence because "[a]ny officer or agent of the corporation who has the power to cause the branch records to be sent from a branch to the home office for any corporate purpose, surely has sufficient control to cause them to be sent on when desired for a governmental purpose properly implemented by a subpoena").

114. *See infra* Part II(B)(5) (discussing how the analysis in this article intersects with E.U. terms of data "controller" and data "processor").

In contrast, where there is limited or non-existent access to a system or data, even where there is a possibility of access, there may not be sufficient evidence of day-to-day control. [115] Consider in this case that the U.K. entity maintains a database that contains data relevant to the services the U.S. entity is contracted to provide. Under the terms of the contract, the U.S. may have access to that database in order to perform its services, but in practice it has never accessed that database. In this case, it is far less likely that the U.S. company would be found to have control over that database, as the U.S. company does not in fact have day-to-day control over the data.

From these examples, one can envision a continuum of possible day-to-day control: on one end, a situation where there is no factual evidence that the data in question has ever been handled, and on the other, strong evidence that the data is handled daily in the ordinary course of the U.S. company's business. Judges would then need to analyze the facts available to determine where along this continuum any specific case falls, weighing the totality of the circumstances to determine if such a finding is sufficient to establish control, as depicted in Figure 7 below.

Figure 7:
Example of a Day-to-Day Control Continuum



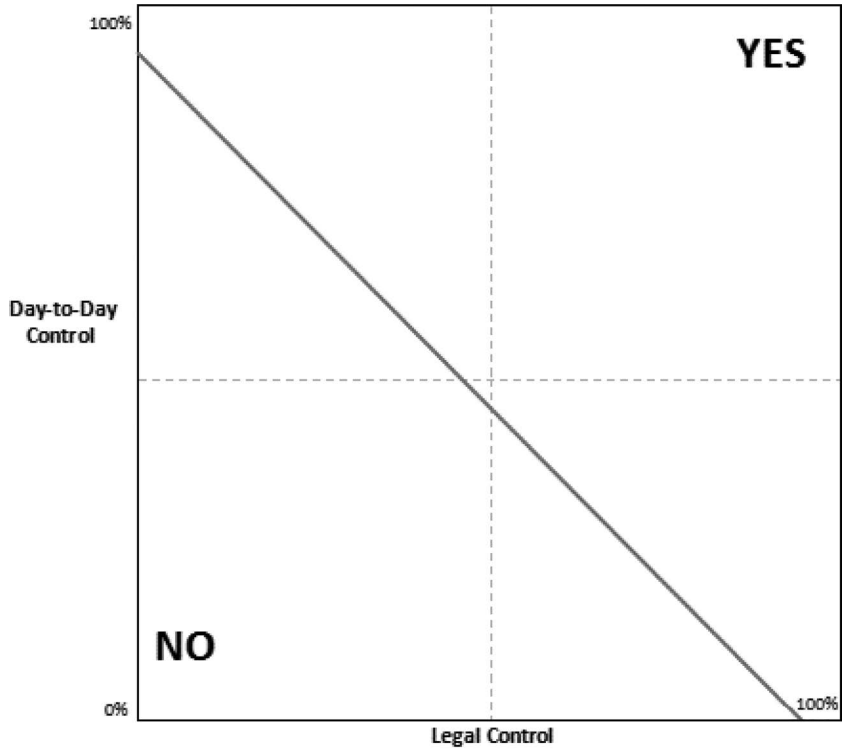
115. *See* Zenith Elecs., LLC v. Vizio, Inc., No. M8-85, 2009 U.S. Dist. LEXIS 90896 (S.D.N.Y. Sept. 21, 2009) (holding that the existence of a parent-subsidiary relationship alone is not sufficient to show control where the subsidiary did not have the ability to access the parent's documents in the ordinary course of business and the two companies maintained separate books); Pitney Bowes, Inc. v. Kern Int'l, Inc., 239 F.R.D. 62 (D. Conn. 2006) (explaining that the U.S. company did not have control over information belonging to a foreign parent in part because the documents were not necessary for the defendant's business or routinely provided to it in the normal course of business).

5. Mixed Legal Control With Day-to-Day Control

By separately analyzing legal and day-to-day control, we can picture how these two aspects of control fit together. Until now, the analysis has focused on when there is sufficient control based on only one of the two criteria. Next, consider Figure 8, where there is some evidence of legal control combined with some evidence of day-to-day control. Beginning at the lower right of the diagram, there is an overall finding of control with a high level of legal control, even with no evidence of day-to-day control. As additional evidence exists about day-to-day control, then not as much legal control may be required to create an overall finding of control. Similarly, at the top left of the diagram, overall control may be found where there is a high level of day-to-day control, even with zero legal evidence of legal control. With evidence of more legal control, less day-to-day control is needed to reach an overall judgment that control exists.

Put another way, it is easier to establish overall control towards the top right of the diagram, where there is strong evidence of *both* legal control and day-to-day control. A court would likely not find control, however, in the bottom left of the diagram, with weak evidence of *both* legal and day-to-day control. In conclusion, Figure 8 is identical to Figure 2 (in the Introduction to this article), providing an overall diagram for when courts are likely to find control.

Figure 8:
Mixed Legal and Day-to-Day Control



B. Four Issues Impacting "Possession, Custody, or Control"

While the framework of the Federal Rules provides helpful guideposts for how courts have interpreted "possession, custody, or control" previously, the CLOUD Act also includes additional considerations. This section will examine four issues that will impact the interpretation of "possession, custody, and control." First, it will look at how the role of corporate structure may or may not impact courts' analysis of "possession, custody, or control." Second, it will examine how the Rules have traditionally applied "possession, custody, or control" differently depending on whether or not the target is a party to the case at hand, and how that issue translates to the CLOUD Act and electronic service providers. Third, it will look at the doctrine of "piercing the corporate veil," and how the doctrine's application differs in evidentiary and non-evidentiary contexts. Finally, this section will explain how "control" for purposes of the CLOUD Act differs from the concept of a "data controller" in European data protection law.

1. The Role of Corporate Structure

The case law demonstrates that corporate structure is a factor courts have considered in determining whether an entity has "possession, custody, or control" of information targeted in discovery or by a subpoena. While a court will also consider other factors in this determination, these cases suggest that a subsidiary does not by definition have "possession, custody, or control" of documents held by its parent company.[116] Instead, a finding of control relies on case-specific facts, including whether the subsidiary has legal or day-to-day control over the data at issue. Important factual considerations include whether the subsidiary has access to the parent's documents in its regular course of business, shares interlocking management structure or shareholders with its parent, or handles the documents on the parent company's behalf while acting as the parent's agent. Courts may rely on these or other factual scenarios to support a finding that a subsidiary has control over data held by a parent company, and therefore can be required to produce it pursuant to the CLOUD Act.

Yet, the Department of Justice has suggested that corporate structure is a non-factor in determining "possession, custody, or control" under the CLOUD Act. In its White Paper, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," the DOJ states that "[t]he CLOUD Act does not alter traditional requirements for jurisdiction over an entity with possession or control over data. The analysis remains the same

116. *See* Gerling Int'l Ins. Co. v. Comm'r of Internal Revenue, 839 F.2d 131, 139-41 (3d Cir. 1988) (explaining that a subsidiary did not have control over documents held by its foreign parent corporation even though the two entities shared a common executive, because that person did not have power over information held by the parent corporation "for the benefit [of the subsidiary]"); Afros S.P.A. v. Krauss-Maffei Corp., 113 F.R.D. 127 (D. Del. 1986) (explaining that the subsidiary entity had control over documents held by its parent entity because the subsidiary was the exclusive seller of the parent's products in the U.S.).

regardless of corporate structure.[117] Respectfully, we disagree with the DOJ's assertion about corporate structure, based on the case law previously discussed.

While the jurisprudence related to the Rules certainly does not suggest that corporate structure is **determinative** of whether an entity has possession, custody, or control, courts have considered it as a contributing factor to the analysis.[118] Yet, where corporate structure is analyzed, it has been in conjunction with additional evidence of the target entity's legal or day-to-day control over the data at issue.[119] Importantly, this analysis is in fact similar to the DOJ's assertion, if DOJ's assertion is understood as stating that corporate formalities *alone* are not sufficient to establish "control" over data belonging to a parent company. Where there is a parent organization and a subsidiary, the courts have established that the information held by the subsidiary is under the parent's control. Where the subsidiary is the targeted entity, the courts have gone further in requiring additional evidence of control over the parent corporation's information, such as through application of the "alter ego" doctrine. In other words, while the DOJ is correct that corporate structure does not alone determine the relevant analysis, corporate structure has been one of the relevant factors considered by the courts.

2. Electronic Service Providers: Parties vs. Non-Parties

One of the factors that influences courts' analysis of "possession, custody, or control" under the Rules is whether the targeted entity is a party to the case at hand.[120] In the context of the Rules, courts appeared more likely to require the production of data where the target entity was a party to the case. This lower threshold for establishing "possession, custody, or control" for parties makes sense given the inherent incentives for one party to a case to resist efforts that would assist the opposing party. A party is more likely to attempt to avoid producing data that would reduce that party's chances of winning, including obfuscating the degree to which it has legal or day-to-day control over the data sought.

A similar rationale would apply to criminal investigation contexts like the CLOUD Act. Where the entity being requested to turn over data is the target of a criminal investigation, the target would have an incentive to resist responding to otherwise valid legal process, including by arguing that it does not have

117. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 17 (Apr. 2019), https://perma.cc/4WSV-CBD5 (emphasis added).

118. *See* Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc. 233 F.R.D. 143, 145 (D. Del. 2005) ("Further, the separate and distinct corporate identities of a parent and its subsidiary are not readily disregarded, except in rare circumstances justifying the application of the alter ego doctrine to pierce the corporate veil of the subsidiary" (citing *Gerling*, 839 F.2d at 140)).

119. *See, e.g.*, Orthoarm, Inc. v. Forestadent USA, Inc., No. 4:06-CV-730-CAS, 2007 U.S. Dist. LEXIS 44429 (E.D. Mo. June 19, 2007); *In re* Uranium Antitrust Litig., 480 F. Supp. 1138 (N.D. Ill., 1979).

120. *See* Jordan, *supra* note 100, at 190; Lori G. Cohen et al., *The Global Courtroom: Discovery of Foreign Documents in U.S. Products Liability Litigation*, A.B.A. (Nov. 16, 2017), https://perma.cc/4XWA-2L7P.

"possession, custody, or control" over the data. A broad interpretation of the phrase also reduces the potential benefits of attempting to "hide" electronic evidence outside the U.S., including storing the data in the name of a foreign-based shell company, both to complicate legal analysis of the CLOUD Act and to potentially introduce additional conflicts of law. In this case, it stands to reason that courts will treat targets of investigations similar to parties to a case, and apply "possession, custody, or control" more broadly.

This rationale also suggests that there could be a narrower interpretation of the phrase when the target is not under investigation. In these cases, the service provider would not have the same inherent incentive to obfuscate the nature of its relationship to the data. To the extent that a service provider raises challenges to such process, including attempts to quash a subpoena on principles of comity, courts may well require a higher level of proof before ordering service providers to turn over data.[121]

3. "Piercing the Corporate Veil" in Evidence vs. Non-Evidence Contexts

There are strong policy reasons to suspect courts will be more likely to "pierce the corporate veil" for purposes of finding "possession, custody, or control" under the CLOUD Act compared to when that term of art is used in the corporate payments or obligations context. In the corporate liability context, one of the core purposes of the fundamental structure of a corporation is to have limited liability, and that limited liability is a central decision factor in how investments are made throughout a set of corporate holdings.[122] This reasoning supports why the business judgment rule largely shields corporate decision makers from personal liability for company losses due to errors in decision making. Instead, courts tend to "pierce the veil" only when there is a violation of a duty of loyalty, such as engaging in self-dealing.

Additionally, if piercing the veil for liability purposes were easier, thereby making the risk of owner liability greater, there would be a significant impact on the expenses for corporations to make investments in companies, reducing the overall flow of capital. Increasing the potential risk to a business's owners would lead owners to be more risk-averse in their decision-making on when to supply capital. Since free-flowing capital is central to our economic system, piercing the veil in this context is an exception rather than regular practice, so as to avoid overly restricting inter-company loans.

In the document production context, however, the policy concerns would appear to be significantly different, warranting a lesser burden of proof in order to

121. In the authors' discussion with DOJ officials, it was explained that DOJ policy is to obtain evidence directly from the owner of the data, and not from a third-party service provider, where possible.

122. *See* Robert B. Thompson, *Piercing the Corporate Veil: An Empirical Study*, 76 CORNELL L. REV. 1036, 1039 (1991) ("The possibility that the failure of a business would allow its creditors to reach all of an investor's nonbusiness assets might deter a risk-averse investor from investing, even though that possibility is small and the investment has a positive net present value.").

have the subsidiary produce evidence held by a parent or other related corporation. Finding common control of documents between a subsidiary and its parent does not directly impact the free flow of capital, and does not have any similar impact on the underlying economic system as a whole. In addition, courts have often noted the vital societal interest in pursuing criminal investigations, supporting a finding that a subsidiary should be obligated to produce documents legally held by a parent or other affiliated corporation.[123]

An example of this analysis is *Power Integrations, Inc. v. Fairchild Semiconductor International, Inc*. There, the court found that corporate formalities separating parent and subsidiary can be *evidence that* the subsidiary does not control documents held solely by its parent, thought it might be *outweighed by mitigating factors* suggesting that the entities do not in fact operate separately in the ordinary course of business as related to the documents at issue.[124] This approach shows that piercing the corporate veil to reach documents needed for a criminal investigation is easier than in cases piercing the veil to receive funds from the owner.

4. Why "Possession, Custody, or Control" in U.S. Law is Different From Being a "Data Controller" Under the GDPR

We seek next to avoid confusion in legal terminology between the term "control" under U.S. law and "controller" under the law of the European Union (and other jurisdictions). We emphasize, especially for those outside of the U.S., that the two terms are entirely distinct. The article thus far has focused on the interpretation of a term of art in U.S. law – "possession, custody, or control" – concerning contested access to evidence. The legal issue is whether an entity has sufficient "control" over a document or other evidence, so it must turn over that evidence to a prosecutor or judge.

This legal analysis is entirely different from a key issue in European Union data protection law, whether a particular entity is a data "controller" or a data "processor."[125] Under the EU approach, a controller is an entity that "determines the purposes and means of the processing of personal data."[126] By contrast, a "processor" is an entity "which processes personal data on behalf of the controller."[127] For instance, one company (the controller) might hire a company to provide computer services on its behalf (the processor). The controller would make decisions, for instance, about whether and when an individual's data should be shared for marketing purposes.

---

123. *See, e.g.*, United States v. Potter, 463 F.3d 9, 25 (1st Cir. 2006) (reasoning that a corporation can be held responsible for the actions of its agents where one of the agents' motivations is to benefit the corporation).

124. *See* Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc., 233 F.R.D. 143, 145 (D. Del. 2005).

125. *See* GDPR, *supra* note 81, art. 4.

126. GDPR, *supra* note 81, art. 4(7).

127. GDPR, *supra* note 81, art. 4(8).

The difference in the terms is easy to see in *Peninsula Hospital v. Xerox State Healthcare, LLC*. In that case, the defendant Xerox was working on behalf of a client, the state of Alaska.[128] The state of Alaska objected to having evidence turned over. The court, however, found that the hospital had "possession and custody" of the data, and thus had to produce the evidence. Under the EU approach, the state of Alaska would have been the "controller," with the hospital processing data on its behalf. Yet, for purposes of U.S. litigation, the records were available to the hospital, which had "possession, custody, or control," and the evidence had to be produced. In short, the hospital was a "processor" in EU terminology, but had "control" for purposes of U.S. evidence law.

In conclusion, under EU law, the term "controller" is tied to the act of deciding what may be done with personal data. The U.S. term of "control," by contrast, focuses on whether there is sufficient legal or day-to-day control over the data to require the company to produce the evidence.

III. COMPELLING PRODUCTION OF EVIDENCE IN OTHER COUNTRIES – A BELGIUM CASE STUDY

Thus far, the article has discussed the U.S. law for compelling production of evidence that is stored abroad. In the face of critiques that U.S. law is too broad, the DOJ has countered that U.S. law is consistent with international norms and the practice in multiple other countries.[129] This Part discusses Belgium as a case study for how the issue is treated elsewhere. In sum, Belgium is at least as broad as the U.S. in requiring production of evidence held abroad by service providers. In two high-profile cases, involving Yahoo! and Skype, Belgium has required production after lengthy litigation with service providers who sought to object to government requests. Belgium has not required a showing that the local business entity have possession, custody, or control over the data; instead, Belgian prosecutors and investigating judges[130], followed by Belgian courts, have considered it sufficient if the company is simply offering services within the country, even where the company has no business office in Belgium. Here, we explain

128. Peninsula Hosp. v. Xerox State Healthcare, LLC, No. 3:15-CV-000177-TMB, 2019 WL 1873297, at *9 (D. Alaska Feb. 5, 2019) ("The Court finds that three of these issues—financial responsibility in the event of a breach, notification of attempted hacking or security breaches, and return of the copied database—are substantially resolved by the Court's decision that Conduent should makes [sic] onsite access available for South Peninsula's expert rather than providing a copy of the database. Conduent will thus retain substantial control over security measures and the database itself, or any copy thereof, such that there will be no need to guard against a breach.").

129. U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT (Apr. 2019), https://perma.cc/SLD5-K62Y; *see also* Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS 2-3 (May 23, 2012), https://perma.cc/DL4C-A6DA.

130. In the Belgian inquisitorial system, investigation is usually directed by the prosecutor, and in certain more complex cases, by an investigating judge. After the investigation is finished, the case could be either closed or referred to court for trial. *See Rights of Victims of Crime in Criminal Proceedings – Belgium*, EUROPEAN E-JUSTICE PORTAL, https://perma.cc/6VKY-4HBC.

Belgium's relevant statutes, discuss the two cases, and highlight similarities and differences between the U.S. and Belgian approaches.

A. Approach in Belgium and the Ability of Belgian Law Enforcement Authorities to Require Production of Information Stored Abroad

This section examines the relevant Belgian statutes, as well as the Yahoo! and Skype cases.[131]

1. Overview of Belgian Legal Provisions Relevant to Production of Electronic Evidence

The Code of Criminal Procedure in Belgium, the general criminal procedural law, has provisions governing the process for prosecutors and judges to seek electronic information and order searches of computers.[132] Certain types of data and searches can be directed by prosecutors themselves on their own authority while for other kinds of searches, an order of the investigating judge is required. In this section, we briefly discuss the relevant provisions that enable such orders.

A prosecutor can seek a "local search" of a computer system by issuing an order on the prosecutor's own authority.[133] Such a search is limited to information on a particular computer system. If a search is to extend beyond the computer to other computers or networks, an order of an investigating judge is required.[134] The latter type of search can be carried out even where the data does not appear to be located in Belgian territory. The data can still be copied and the investigating judge is required to inform the Ministry of Justice, which would inform the authorities of the state concerned, where it can be reasonably determined.[135] This is useful to note since it appears to authorize collection of evidence stored beyond local territories.[136]

The Code also sets out powers of prosecutors and judges to seek the assistance of service providers in obtaining evidence, with specific provisions concerning subscriber information, traffic data, and the content of communications.[137] A

131. The authors thank Mona Giacometti for her assistance with the discussion of Belgian law. Ms. Giacometti is a Belgian lawyer who is completing her doctoral dissertation at the Université Catholique de Louvain-la-Neuve on issues of cross-border access to e-evidence.

132. *See* CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] (Belg.).

133. *Id*. art. 88ter. Also, if access to the device is not password protected, the police can execute the local search on their own without the need for a prosecutor's order.

134. *Id*. *reintroduced by* Act of May 5, 2019, art. 11. Article 88ter was repealed on December 25, 2016 to enable prosecutors to order extension of a search. This was, however, overturned by the constitutional court of Belgium by a decision on December 6, 2019.2018 (case n° 2018/174). The provision has subsequently been reintroduced by the Act of May 5, 2019.

135. *Id*.

136. In other cases (for instance, a remote search), an order of an investigative judge is required as well. *Id*. art. 90ter. These other cases can also involve an extension of the search. However, the person in charge of the computer system need not be informed while for searches ordered under articles 39bis & 88ter, such notice is required. *Id*. art. 39bis, § 7.

137. The Georgia Tech research team has previously compared the approaches of France and the U.S. for government access to information held by service providers. *See generally* Peter Swire et al., *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323 (2017).

prosecutor can request the cooperation of an "operator of an electronic communication network or a provider of an electronic communication service" to obtain "identification data" (or subscriber information, as it is commonly known in the U.S.), through a reasoned and written decision.[138] The decision should reflect proportionality of the measure with the privacy of individuals and its subsidiarity in relation with other less intrusive investigative measures. For obtaining traffic data or location of origin or destination of communication, an order of an investigating judge is required—an investigating judge can require technical assistance of an operator or a provider of an electronic communications service for obtaining such data.[139] In requesting such assistance, the investigating judge has to record a reasoned order indicating the circumstances which justify the measure and its proportionality with regard to respect for private life and its subsidiarity in relation with other less intrusive investigative measures.[140] A service provider's cooperation can also be required to obtained content data.[141] Failure to comply with the request can be punished with a fine.

These provisions set the background for the discussion on two cases where non-Belgian service providers were asked to cooperate with prosecutors and judges in obtaining data.

2. The Yahoo! Case

In the Yahoo! case, after extensive litigation, the court compelled Yahoo! to produce the requested evidence from U.S.-registered accounts. In 2007, the public prosecutor of Dendermonde requested Yahoo! Inc, U.S. to provide identification information relating to specific email accounts.[142] The request was sent to Yahoo! Inc's offices in the U.S. (Yahoo! does not have a local office in Belgium). The information requested was identification/registration data of the persons who created the account, including IP addresses, date and hour of registration, the email address connected with the profile, and all other personal data or information that could lead to identification of the account user. Yahoo! refused to comply stating that the requested information concerned U.S.-registered accounts and under ECPA, such information could not be transmitted without a claim to this effect from a U.S. jurisdiction. In their view, such a request had to be made through the U.S. DOJ pursuant to the MLAT.[143]

The case was first brought by the prosecutor before the Court of First Instance of Dendermonde, where the court ordered Yahoo! to pay a pecuniary penalty of 10,000 Euros for failing to comply with the prosecutor's order.[144] Yahoo!

138. CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] art. 46bis (Belg.).

139. *Id*. art. 88bis.

140. *Id*.

141. *Id*. art. 90quater, § 2.

142. Pursuant to its authority under Article 46bis of the CODE D'INSTRUCTION CRIMINELLE [C.I.CR.] (Belg.).

143. Public Prosecutor v. Yahoo! [Civ.] [Tribunal of First Instance] Dendermonde, Mar. 28, 2009, TIJDSCHRIFT VOOR STRAFRECHT [T.STRAFR.] 2009, 116 (Belg.).

144. *Id*.

appealed to the Court of Appeals and to the Court of Cassation,[145] where the case was brought three times before the final ruling in 2015.[146]

Yahoo! argued that the public prosecutor did not have territorial jurisdiction since Yahoo! was neither an operator of an electronic communications network established in Belgium nor a provider of an electronic communications service established in Belgium. The company argued that it was not present in Belgium in any way and that placing sanctions on the company to enforce the obligation of cooperation would be an exercise of unlawful extraterritorial jurisdiction. Instead, to obtain the requested information, the public prosecutor was required to follow the procedure stipulated in the agreement for mutual legal assistance (MLAT) between the U.S. and Belgium.

Yahoo!'s arguments were finally rejected by the Belgian Court of Cassation. The Court of Cassation noted that a State could impose a measure of coercion, like the one envisaged under Article 46bis, on its own territory. Where there was a sufficient territorial link between the measure and the territory, the State was imposing the measure on its own territory and not exercising extraterritorial jurisdiction.[147] The nature and scope of the coercive measure helped determine the territorial link. In this case, the measure intended to enforce upon operators and suppliers "active in Belgium" a request to obtain subscriber information during an investigation which fell within the competence of the Belgian prosecutors. This did not require presence of Belgian authorities or their agents abroad.[148] The measure applied to every operator or supplier "that directs his economic activity on consumers in Belgium."

The Court of Cassation found that Yahoo! was present on Belgian territory and had voluntarily subjected itself to Belgian law. In the Court's view, Yahoo! actively participated in Belgian economic life on account of the following: (i) the specific use of the domain name 'www.yahoo.be', (ii) the use of local language; (iii) showing advertisements based on the location of the users of its services; and (iv) Yahoo!'s reachability in Belgium for these users by installing a complaint

145. The Court of Cassation is the highest court in Belgium. *See* EUROPEAN LAW INSTITUTE, https://perma.cc/W7TL-DCCB ("The Court of Cassation is the main court of last instance in Belgium. It reviews the lawfulness of judicial rulings but does not review the facts of cases as they have been determined by lower courts. As such, the aim of the Court is to safeguard legal uniformity and the development of the law.").

146. *See* Paul de Hert et al., *Legal Arguments Used in Courts Regarding Territoriality and Cross-Border Production Orders: From Yahoo Belgium to Microsoft Ireland*, 9 NEW J. EUR. CRIM. L. 326, 18 (2018) ("The case took a challenging road through the courts starting in 2009 at the Criminal Court in Dendermonde, being subsequently appealed at the Court of Appeals in Ghent in 2010, running further up the judicial ladder to the Court of Cassation (2011), from there being referred to the Court of Appeals in Brussels (2011), again up to the Court of Cassation (2012), from where it was finally referred to the Court of Appeals in Antwerp (2013) and ultimately brought in front of the Court of Cassation for the third and final time in 2015.").

147. Public Prosecutor v. Yahoo!, Inc., Hof van Cassatie [Cass.] [Court of Cassation] [Supreme Court of Belgium], Dec. 1, 2015, No. P.13.2082.N, ¶¶ 4-5 (Belg.).

148. *Id.* ¶ 6.

box and an FAQ desk.[149] We note that there was no requirement that the investigating judge show that Yahoo! controlled the evidence from within Belgium – the evidence had to be produced even though Yahoo! did not have any office in the country.

3. The Skype Case

In 2012, an investigative judge in the Mechelen ordered wiretapping of an individual's Skype account. The order for wiretapping was accompanied by a request for technical assistance pursuant to Articles 88bis and 90quater of the Belgian Rules of Criminal Procedure. The request for technical assistance was addressed to Skype, established in Luxembourg, and if necessary, with the assistance of the parent company Microsoft Corp, and was sent to Skype through an email. In response, Skype only produced registration information relating to the Skype account, and in several emails, responded noting that it did not store such data and that communications content was encrypted. It also noted that user data was owned and retained by Skype Communications SARL in Luxembourg and was subject to Luxembourg law—if any request was to be made for data outside the scope of data that Skype could voluntarily share with law enforcement, the Belgian authorities would need to follow the MLAT process.

A case was brought against Skype for failing to provide technical assistance, for which sanctions could be imposed on it under Sections 88bis and 90quater of the Belgian Criminal Procedure Code. Skype argued that it did not fall within the scope of these provisions. In Skype's view, since it was established in Luxembourg and not Belgium, the liabilities resulting from those provisions were not applicable to it. Skype also argued that the offence for which it was being prosecuted did not have any link with Belgian territory—the company was established in Luxembourg as per Luxembourg law and had no separate establishment in Belgium.

The Court of First Instance in Mechelen[150], followed by the Court of Appeal in Antwerpen[151] found that Skype was a supplier of telecommunication service within the meaning of articles 88bis and 90quater[152] – since it provided technical means to users in the form of software to communicate and exchange information

149. *Id.* ¶ 9.

150. Public Prosecutor v. Skype [Civ.] [Tribunal of First Instance] Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12 (Belg.).

151. Public Prosecutor v. Skype [Civ.] [Court of Appeal] Antwerp, Nov. 17, 2017, NIEUW JURIDISCH WEEKBLAD [NJW] 78 (Belg.).

152. It may also be noted that at the time, Articles 88bis and 90quater applied to "telecommunication network operators" and "suppliers of telecommunication service" unlike Article 46bis which applied to "operator of an electronic communication network" and "supplier of an electronic communication service." Before 2007, Article 46bis also used the term telecommunication provider and operator instead of electronic communication. It was amended in 2007 to clarify ambiguity regarding whether a request sent to a provider of electronic communications to identify an IP address could only be ordered by an investigating judge and not prosecutor (under Article 46bis). The difference in the terms used was not intentional.

through an electronic network with other users. On the question of presence in Belgium, the Mechelen court referred to the Court of Cassation's ruling in the Yahoo! case, reiterating that the execution of the request did not require the presence of police or agents abroad, nor was any act required to be taken place abroad. The obligation to make available the necessary information, data, and technical assistance was considered to be complied with on Belgian territory, and there was no intervention required outside Belgium.

To be subject to a coercive measure, sufficient territorial link was required and following Yahoo!, such link could be found by active participation of Skype in Belgian economic life, even if there was no registered office or establishment in Belgium.[153] The court found that Skype had made its software available to users on Belgian territory and the suspect (whose information was requested) could make use of the software to communicate from Belgian soil with others. The court also noted that Skype's website was accessible in Dutch, user manuals were available in Dutch, and users could get support in Dutch for troubleshooting. Also, there appeared to be "focused advertisements in function of the place where the user stays, his language preference and the location of the IP-address."[154] The Court imposed a fine of 30,000 Euro on Skype as sanction.

On appeal, the Court of Appeals in Antwerp upheld the Mechelen Court's decision. The Court found an economic presence in Belgium which transcended "mere 'virtual' presence via a (passive) internet site."[155] In the Court's view, for a company to be economically active, a registered office or place of business was not essential. It would be sufficient if the company had the intention of concluding contracts with Belgian customers. Skype offered different countries, and specifically Belgian users, several ways to pay for the services. Following the Mechelen Court's reasoning, the court also reiterated the accessibility in Dutch and focused ads[156] as facts that indicated Skype's active participation in Belgian economic life.

153. Public Prosecutor v. Skype [Civ.] [Tribunal of First Instance] Mechelen, Oct. 27, 2016, No. ME 20.4.1 105151-12, ¶ 5.3.4 (Belg.) ("As to the assessment of the obligation to cooperate, it is therefore not the location of the registered office or establishment that is decisive, but the place where the service supplier offers his services.").

154. *Id.* ¶ 5.3.5.

155. Public Prosecutor v. Skype [Civ.] [Court of Appeal] Antwerp, Nov. 15, 2017, NIEUW JURIDISCH WEEKBLAD [NJW] No., ¶ 5.1.2.2 (Belg.) ("SKYPE had provided a Dutch version of its website so that Dutch-speaking Belgian users could use SKYPE's services in Dutch automatically (either through their IP localisation or through their choice of language from an Internet browser, at least as of December 2012), which can only be explained by SKYPE's clear desire to actively and commercially address potential users of SKYPE's technology in Belgium. If SKYPE did not intend to actively target the (Dutch-speaking) Belgian market, there was no reason to also provide a Dutch version of its website." (unofficial translation)).

156. Skype argued that it did not display advertisements since this was outsourced to Microsoft. The Court noted that Belgian Skype users did see ads when using its software and the fact that the locally relevant ads were not placed by Slype itself but by its parent company, did not alter the fact that Skype was also economically active on Belgian territory.

B. Similarities and Differences With the U.S. Approach of Requiring Information Within the Provider's Possession, Custody or Control

The Yahoo! and Skype cases have clarified the Belgian position with regard to seeking cooperation from service providers and requiring production of evidence. Similar to the CLOUD Act, location of the evidence has not been determinative. Instead, the question was whether a service provider with no physical presence in Belgium was within the reach of Belgian prosecutors and courts. The courts found that as long as there was sufficient territorial link between the cooperation sought and Belgian territory, service providers could be asked to cooperate. A court could find territorial link by assessing whether the service provider was active in Belgium, for which actual physical location in the form an office was not necessary. Following the 2015 Court of Cassation ruling in the Yahoo! case, the Belgian Criminal Procedure Code was amended to clarify the language and reflect this understanding.[157] Once such territorial link was found, a service provider could be asked to cooperate and produce information.

The Belgium cases focused on issues of personal jurisdiction, whether the company was present on Belgian territory and had voluntarily subjected itself to Belgian law. This approach is similar to the U.S. DOJ's approach of requiring entities that are subject to its personal jurisdiction to produce information. In the *Marc Rich* case, the corporation was a Swiss corporation and on finding that the company was subject to U.S. courts' personal jurisdiction, it was compelled to produce information regardless of its location.[158] When the DOJ sought evidence from Microsoft, it was indisputable that the U.S. had jurisdiction over Microsoft and that Microsoft offered services in the U.S.

The principal difference appears to be that the U.S., as stated in the CLOUD Act, requires an additional finding before the company must produce the evidence. Not only must there be personal jurisdiction, but the U.S. court must also find that there is "possession, custody, or control" of the evidence within the U.S. The company that receives a request for evidence can dispute the order even where personal jurisdiction exists, if the requisite facts showing control are absent.

This examination of Belgian law is consistent with statements of DOJ that "U.S. law complies with long-standing international principles already implemented in many countries," with Belgium and 10 other countries cited as "asserting domestic authority to compel production of data stored abroad."[159] Contrary

157. *See generally* Loi portant des modifi cations diverses au Code d'instruction criminelle et au Code pe¨nal [An Act to amend the Code of Criminal Procedure and the Penal Code] of Dec. 25, 2016, MONITEUR BELGE [M.B.] [Official Gazette of Belgium], 2738.

158. *See supra* Part I(A)(2).

159. The DOJ has stated: "Australia, Belgium, Brazil, Canada, Colombia, Denmark, France, Ireland, Mexico, Montenegro, Norway, Peru, Portugal, Serbia, Spain, the United Kingdom, and other countries assert domestic authority to compel production of data stored abroad." U.S. DEP'T OF JUSTICE, PROMOTING PUBLIC SAFETY, PRIVACY, AND THE RULE OF LAW AROUND THE WORLD: THE PURPOSE AND IMPACT OF THE CLOUD ACT 6 (Apr. 2019), https://perma.cc/SLD5-K62Y. The statement of the Department of Justice – that many countries assert the authority to compel production of data stored

to European critics of the CLOUD Act who consider it extraordinary that the U.S. government can access evidence stored abroad, the Belgian cases show a European nation that also requires access to evidence stored abroad, even for companies with no business office in the country.

CONCLUSION

Much like the introduction of MLATs in 1977, the CLOUD Act has given U.S. law enforcement a clearer path to accessing electronic evidence stored outside the U.S. While the CLOUD Act lacks a statutory definition of "possession, custody, or control," that phrase's appearance in the Federal Rules of Civil and Criminal Procedure has created a foundation of jurisprudence examining how to define that phrase. That foundation suggests that the heart of future conflicts will be around whether an entity has "control" over evidence sought, as actual "possession" and "custody" are less ambiguous to establish. While it is nearly impossible to set bright line rules for what will establish control, or a lack of control, for purposes of the CLOUD Act, the Rules and public policy considerations suggest a few key issues will likely influence courts' decisions.

First, the analysis of "possession, custody, or control" will likely be fact-specific, and based on the totality of the circumstances. For instance, corporate structure will be one of the factors considered, but will not be determinative of whether or not there is control. In other words, courts will factor in that a subsidiary is a separate entity from its corporate parent, but may still find the subsidiary has control over data held by the parent if the subsidiary has enough day-to-day control over the data.[160]

Second, public policy interests suggest that courts will be more likely to "pierce the veil" and attribute control to a target entity over data held by a corporate relative when one of those two entities is the target of an investigation. Unlike in corporate finance contexts, courts need not worry about restricting the flow of capital and hampering business activities based on how they interpret "possession, custody, or control" under the CLOUD Act. Indeed, in this type of evidentiary context, the goal of investigating crimes supports an approach where bad actors are not incentivized to hide evidence outside the U.S. by falsely demonstrating a lack of "possession, custody, or control," or to introducing potential conflicts of law.

Finally, stakeholders in the U.S. and abroad should be careful not to conflate "data controllers" with the CLOUD Act's application of the term "control."

---

abroad – is consistent with our research. The Department of Justice also makes an additional statement, that this authority to compel production "is required by the Budapest Convention." *Id*. Eleni Kyriakides has argued that the authority is not required by the Budapest Convention. Eleni Kyriakides, *Critiquing DOJ's Claim that the Budapest Convention Requires the Cloud Act's Solution*, CROSS-BORDER DATA FORUM (July 9, 2019), https://perma.cc/2VVF-NPXZ. We take no position on whether the Budapest Convention requires this authority.

160. There may be reasons that a subsidiary has legal control over data, even with respect to data held by the parent. For instance, a contract may exist giving the subsidiary a legal right to access the data.

Merely setting up a related U.S. entity as a "data processor" will not on its own establish that the U.S. entity does not have "possession, custody, or control" of the non-U.S. company's data for purposes of the CLOUD Act. Courts will look to all of the relevant facts in determining whether a company has legal or day-to-day control over the data sought. Likewise, a finding of "control" under the CLOUD Act does not make the entity a "data controller" for purposes of the General Data Protection Regulation. The two analyses are separate and distinct, and while they may look at similar factors, one determination does not control the other.

Despite these issues, however, stakeholders should find some comfort that the history of the Rules well help guide courts' analysis of the CLOUD Act. Given the similar evidentiary contexts between the Rules and the CLOUD Act, the inclusion of the same term of art without an accompanying statutory definition, and the incentive for courts to avoid interpreting the same phrase differently in related contexts, the jurisprudence around the Rules will likely influence the interpretation of the CLOUD Act. If courts follow the history of the Rules, then analysis under the CLOUD Act will largely focus on whether the facts demonstrate that the targeted entity has legal or day-to-day control over the evidence sought, regardless of where the evidence is physically stored.

***