CRi
Computer Law Review International
A Journal of Information Law and Technology

Articles

*Paul Schwartz / Karl-Nikolaus Peifer**

Data Localization Under the CLOUD Act and the GDPR

A Quest for an efficient path to legal certainty

On March 23, 2018, the U.S. Congress enacted the CLOUD Act to resolve the highly anticipated question before the Supreme Court in Microsoft Ireland, regarding the U.S.'s ability to access international cloud data. In one of the most far-reaching changes to U.S. surveillance law in decades, the CLOUD Act establishes the extraterritorial reach of the Stored Communications Act (SCA) in two main steps. Its immediate effect occurs in the law's "Step One," which confirms that the SCA extends internationally. In "Step Two," the CLOUD Act sets up a process for the creation of bilateral executive agreements between the U.S. and foreign governments to provide reciprocal authority to make direct requests for information from cloud providers in the other's jurisdiction. Under both circumstances, the cloud provider may move to quash the order, and the court is to assess the enforceability under a multi-factored comity analysis. These two steps of the CLOUD Act raise important policy issues and point to a need for more coordinated efforts between the EU and the U.S. The CLOUD Act may encourage governments to engage in an arms race for stricter data protection laws and sanctions. It may also encourage companies to localize data storage in the EU. Moreover, the CLOUD Act may be on a collision course with the GDPR. This Article proposes that the most sensible and efficient path to legal certainty for cloud providers would be an accord between the U.S. and the EU itself.

I. Introduction

1 On March 23, 2018, Congress enacted the CLOUD Act, one of the most far-reaching changes to U.S. surveillance law in decades.[1] This statute was passed as the last section of a 2000-page spending bill. The immediate impact of the law has been nonetheless significant: on April 17, 2018, the Supreme Court announced that enactment of this statute mooted the matter of *Microsoft Ireland v. U.S.*

The CLOUD Act resolved the controversy underlying *Microsoft Ireland* by making it clear that the Stored Communications Act (SCA) extends internationally. As a result, U.S. cloud providers worldwide are subject to U.S. orders for data stored in their control, possession, or control, regardless of where the data is stored, if otherwise subject to U.S. jurisdiction. Under the CLOUD Act, providers can also seek to quash these orders in U.S. courts. Specifically, a U.S. provider can claim that obeying the U.S. order will violate laws in their home country or in a foreign country. U.S. courts are to then analyze this conflict of laws pursuant to a comity analysis 2

1. Two Step Approach

Yet, the elements of the statute that extend the extraterritorial reach of the SCA are only part of this important new law. This Article refers to this extension as the CLOUD Act's "Step One." In its "Step Two," the Act sets up a process for the creation of bilateral executive agreements between the U.S. and foreign governments. Although no such agreements are in place yet, such accords will grant the U.S. government the ability to 3

* The authors wish to thank the Berkeley Center for Law & Technology and Microsoft for their research support.

1 Consolidated Appropriations Act, 2018, Pub. L. No. 115-141, Div. V "Clarifying Lawful Overseas Use of Data Act of 2018," §§ 101-106 (2018) [hereinafter CLOUD Act].

make direct requests for information from cloud providers in a foreign jurisdiction and grant the respective foreign government the authority to make similar requests to U.S. cloud providers. The idea is one of reciprocity. These agreements can even permit real time surveillance of the content of communications.

4 The CLOUD Act's bedrock principle of international reciprocity is in alignment with global trends. For example, the Council of Europe's Convention on Cybercrime (2001), also known as the Budapest Convention, seeks to heighten mutual assistance among nations in combating electronic crimes.[2] The Budapest Convention requires signatory nations to set up a central authority who can assist in answering requests for mutual assistance. Its goal is for parties to the Convention to "afford one another mutual assistance to the widest extent possible for the purpose for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."[3]

2. Policy Issues

5 These two steps of the CLOUD Act raise important policy issues. This Article identifies a series of potential collisions ahead between the EU and U.S. following enactment of this law. *First*, the CLOUD Act does not itself qualify as an "international agreement" under Article 48 of the GDPR.[4] As a result, transfers of data from the EU pursuant to SCA orders under the Act's Step One will conflict with EU data protection law. *Second*, executive agreements created under the CLOUD Act's Step Two may fail to provide an "adequate level of protection" as required both by the GDPR and by EU constitutional norms as identified by the CJEU's *Schrems* decision.[5] Thus, the U.S. CLOUD Act has not reduced the uncertainty in this area of international data privacy law.

3. Shift Towards Localized Clouds

6 This unpredictability of legal results provides an incentive to cloud providers to invest in EU localization clouds. Even though the CLOUD Act extends the reach of the SCA beyond the borders of the U.S., the location of the stored data remains relevant to the comity analysis under the CLOUD Act. In particular, under both Step One and Two, localized clouds will be able to make comity arguments that are not available to non-localized clouds in U.S. courts. At the same time, however, localization is unlikely to be a complete solution because the CLOUD Act's comity analysis foresees a decentralized, fact-specific process for deciding contested transfers. Ultimately, the need is for a data sharing accord between the EU and the U.S., instead of the CLOUD Act's bilateral nation-to-nation arrangements. Only this step can avert the coming collisions between EU and U.S. data protection regimes.

II. The CLOUD Act

7 To understand the CLOUD Act, one can first examine the underlying controversy in *Microsoft Ireland* and then turn to the statute itself. This Part will explore the *Microsoft Ireland* litigation and Congress' rapid response to it in enacting the CLOUD Act. *Microsoft Ireland* focused on issues such as significance of where cloud data was located and where a cloud provider would access it upon receipt of a law enforcement order for stored data. These matters still remain of relevancy after passage of the CLOUD Act.

1. The Road to the CLOUD Act: *Microsoft Ireland*

The litigation in *Microsoft Ireland* received worldwide attention. It concerned a warrant that the U.S. government issued to Microsoft pursuant to the Stored Communications Act (SCA), the most important U.S. law governing law enforcement access to cloud data.[6] This warrant related to information associated with an msn.com email. In response to the warrant, Microsoft disclosed all responsive information kept in the U.S., but filed a motion to quash the warrant for e-mail content localized in its Dublin data center. Microsoft viewed itself as obliged to follow Irish law, which required the U.S. government to proceed through the process set up by a Mutual Legal Assistance Treaty (MLAT) with Ireland, and not unilaterally through direct service of U.S. government warrants. The U.S. district court engaged in de novo review and denied the motion to quash.[7] 8

On appeal before the Second Circuit, however, Microsoft was more successful. The Second Circuit held that the SCA did not provide legal authority that extended extraterritorially. As a result, the SCA did not oblige Microsoft to give the U.S. government information stored in its Dublin data center. In the court's view, "[w]hen it passed the Stored Communications Act almost thirty years ago, Congress had as a reference a technological context very different from today's Internet-saturated reality."[8] Recognizing the standard "presumption against extraterritorial application" of statutes that are silent regarding the extent of their reach, the Second Circuit held that execution of the warrant "would constitute an unlawful extraterritorial application of the Act."[9] For the Second Circuit, moreover, it was not important where the data might be *accessed* and disclosed to the government. Rather, the key factor for its consideration was where the information was *stored*. The *Microsoft Ireland* court stated, "Because the content subject to the Warrant is located in and would be seized from the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States."[10] 9

Upon the government's request for a rehearing, the Second Circuit divided 4-4, which meant that the government failed to 10

2 Council of Europe, Convention on Cybercrime, Budapest, Dec. 23, 2001, European Treaty Series No. 185.

3 Id. at Art. 25(1).

4 General Data Protection Regulation, 2016/679, 2016 O.J. (L. 119) 1, art. 48 (EU) [hereinafter GDPR].

5 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (Oct. 6, 2015).

6 18 U.S.C. §§ 2701–2712 (2012) (Stored Communications Act).

7 *In re* Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F.Supp.3d 466 (S.D.N.Y. 2014).

8 Microsoft Corp. v. United States, 829 F.3d 197, 205 (2d Cir. 2016).

9 *Id.* at 209.

10 *Id.* at 220.

gain the majority vote required to revisit the matter en banc.[11] These appellate judges struggled with the competing questions of where the government might be able to access the information as opposed to where it was stored. Moreover, as the dissenters noted, other courts that considered this issue had reached a contrary conclusion and decided that the SCA does have extraterritorial reach.[12]

11 The path to the CLOUD Act was now set. At oral arguments before the Supreme Court on February 27, 2018, Justices *Ruth Bader Ginsburg* and *Sonya Sotomayor* alike both recommended that Congress enact a bill to resolve the matter. In the words of Justice *Ginsburg*, "much time and ... innovation has occurred since 1986," the date of the SCA's enactment, and "if Congress wants to regulate in this brave new world, it should do it."[13] Congress took the hint in March 2018 by enacting the CLOUD Act, and the Supreme Court responded in April 2018 by declaring *Microsoft Ireland* moot.[14] There was now no live dispute remaining between the parties on the issue of whether or not an SCA warrant had extraterritorial reach. The CLOUD Act extended the SCA to information "regardless of whether such information is located within or outside the United States."

2. The CLOUD Act

12 To understand the CLOUD Act, one must consider two of its elements: one that took effect immediately, and another that depends on future action. The first aspect concerns the global extension of the SCA; it is this feature that led to the mooting of *Microsoft Ireland*. The second, which has received far less publicity, is potentially of even greater importance. It sets up a process for wide-reaching executive agreements between the U. S. and other countries to permit data access by U.S. law enforcement to foreign cloud servers, and by foreign governments to U.S.-based cloud services. These executive agreements can also reach beyond stored data alone to permit real time interception of content.

a) Step One

13 The initial aspect of the CLOUD Act is the one on which the Supreme Court relied in dismissing *Microsoft Ireland*. This law amends the SCA to extend the power of the U.S. government to reach data stored extraterritorially. It states that cloud providers are to comply with the provisions of the SCA "regardless of whether such communication, record, or other information is located within or outside of the United States."[15] This provision became operative immediately upon enactment of the law.

14 Upon receiving such an SCA order, a cloud provider located outside of the U.S. is granted recourse to contest the warrant by claiming a conflict of laws.[16] A U.S. court is to resolve the conflict through use of the principle of "comity."[17] This concept leads to the use of a balancing test under which a domestic court decides whether or not to extend courtesy to a foreign jurisdiction by recognizing the validity of its law.[18] As part of extending the SCA extraterritorially, the CLOUD Act provides for a comity analysis pursuant to common law standards when SCA orders are contested.

b) Step Two

15 The second part of the CLOUD Act creates a new way for governments to access cloud data that is relevant for criminal investigations but stored extraterritorially. The key policy concept here is, again, that of reciprocity. Step Two permits the creation and execution of "executive agreements" with "qualified foreign governments."[19] Through these bilateral accords, the U.S. and a foreign government may grant each other the ability to make requests directly of cloud providers in the other jurisdiction. Such requests, however, may be made only for "serious crime," which includes terrorism. This statutory term has been criticized for not being precisely defined.[20]

16 One key statutory term of art in this part of the CLOUD Act is that of the "qualifying foreign government." To fall into this category, a foreign country must offer providers "substantive and procedural opportunities" similar to those provided by the CLOUD Act.[21] These safeguards include permitting a provider to seek to "quash or modify" legal requests for communications. The U.S. cloud provider must also be able to pursue a voiding of foreign orders for data access. In addition to the earlier part of the CLOUD Act, which references common law comity standards, this statute creates a more detailed list of comity factors for use by U.S. courts in judging contested warrants. Moreover, the CLOUD Act contains an important safeguard for transparency in a provision that requires a provider to be able to disclose a legal request for data to the foreign government whose jurisdiction is implicated.

---

11 Microsoft Corp. v. United States, 855 F.3d 53 (2d Cir. 2017) (rehearing en banc denied).

12 *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E. D. Pa. 2017) ("Google Pennsylvania"). Other cases analyzing the Google cloud have reached the same result as *Google Pennsylvania*. *See, e.g., In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017); In the Matter of Search of Info. Associated with [redacted]@gmail.com, No. 16-mj-757, 2017 WL 2480752 (D. D.C. June 2, 2017); *In re* Search of Content that Is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1487625 (N.D. Cal. Apr. 19, 2017).

13 *See* Transcript of Oral Argument, United States v. Microsoft Corp., No. 17-2, 6 (Feb. 27, 2018).

14 United States v. Microsoft Corp., No. 17-2, 584 U.S. _, slip. op. at 6 (vacating as moot).

15 CLOUD Act, *supra* note 1, at § 103(a)(1) (adding 18 U.S.C. § 2713).

16 CLOUD Act, *supra* note 1, at § 103(b) (adding 18 U.S.C. § 2713(h)(2)(A)(ii), providing that a cloud provider may seek to quash a disclosure request for a customer who is not a U.S. person or a U.S. resident and for whom the disclosure of data "would create a material risk that the provider would violate the laws of a qualifying foreign government.").

17 CLOUD Act, *supra* note 1, at § 103(b) (adding 18 U.S.C. § 2713(h)).

18 Hilton v. Guyot, 159 U.S. 113, 163-64 (1895).

19 CLOUD Act, *supra* note 1, at § 105(a) (adding 18 U.S.C. § 2523, "Executive agreements on access to data by foreign governments").

20 *Daniel Sepulveda, Bill on Cross-border Data Access Needs to Change, Despite Laudable Goal*, Hill (Mar. 16, 2018), http://thehill.com/opinion/technology/378785-bill-on-cross-border-data-access-needs-to-change-despite-laudable-goal ("[T]he CLOUD Act should provide greater clarity in what kinds of crimes qualify for use of the authority and transparency in the decision the executive reaches to grant the partner country the new authority ... While there is no international definition for a serious crime, some minimal threshold must be set. Possible thresholds could include crimes carrying a prison sentence of three years or more or some other articulable baseline.").

21 CLOUD Act, *supra* note 1, at § 103(a)(1) (adding 18 U.S.C. § 2713(h)(1)(A)(ii)).

17 A second key statutory term concerns the conditions for and content of the "executive agreements" that must be in place before direct data requests are permitted. Before certifying an "executive agreement," the U.S. Attorney General is to evaluate the domestic law of the foreign government and find that it "affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement."[22] The CLOUD Act also establishes standards for data requests by the qualifying foreign government that are sent to U.S. cloud providers. A request must be particularized, based on "articulable and credible facts," and subject in the foreign jurisdiction to "review or oversight by a court, judge, magistrate, or other independent authority."[23]

18 As a final key concept, the CLOUD Act seeks to restrict the gathering of information by foreign governments about U.S. persons or persons in the U.S. by requiring "targeting" and "minimization" in data gathering. The "targeting" and "minimization" concepts in this part of the law are standards borrowed from the Foreign Intelligence Surveillance Act.[24] This part of the CLOUD Act raises significant privacy issues because, as noted, the anticipated executive agreements can authorize the capturing of real time access to communications, including their content.[25] Legal systems usually grant their highest privacy protections to such data. Recall as well that the CLOUD Act's Step Two requires reciprocity between the U.S. and the foreign government with which an agreement is reached. As part of signing such an accord with the U.S., a foreign government would be required to amend its national surveillance law, if necessary, to permit providers to carry out real time interceptions on behalf of a U.S. government entity.

III. How Does the CLOUD Act Regulate Data Localization Clouds?

19 As we have seen, issues regarding the meaning of data location and data access were a key part of the *Microsoft Ireland* litigation. The CLOUD Act does not end the debate over these concepts, and if anything, complicates it further. The difficulty follows from how data localization will be a future element in the comity analysis carried out by U.S. courts under the CLOUD Act.

1. The Trend Towards Data Localization

20 One of the most important developments in the cloud landscape is the emergence of localized clouds. There have been billions of dollars spent on the creation of localized data centers in Europe. From 2015 to 2016, Microsoft alone invested $1 billion dollars on expanding its cloud offerings in Europe.[26] It has spent a total of $3 billion in this region since 2005. Amazon Web Services has also opened multiple data centers in France, Britain, and other EU Member States. In 2017, Google added a multimillion-dollar complex in the Netherlands, the latest addition to the list of countries where it has data centers. Finally, Apple is opening its first EU data centers in Denmark and Ireland this year. One technology research firm has predicted that the EU market for cloud application services will double by the end of the decade.[27]

An important distinction should be made, however, between data localization as a technical matter and as a legal matter: 21

- *Technical localization* refers to a network configuration that stores digital information exclusively in one location or region and that excludes it from other geographic locations.[28]
- In contrast, *legal localization* refers to a statute or other binding legal mandate that requires such local data storage.[29]

An increased number of countries require data localization as a legal matter. Anapum Chander and Uyen Lê have documented this global trend of legal data localization.[30] Russia and China have particularly strict legal requirements for data localization. In the EU, a more limited example of this trend would be German telecommunications law, which makes certain kinds of data subject to mandatory retention in Germany.[31] In the EU, there is also a high level of customer interest in localized clouds. As one trade publication explains, "[th]e main selling points for cloud operators in Germany are location, location, and location."[32] In a similar fashion, a cloud computing analyst has noted, "Countries like Germany are well aware of data privacy, and it has made them more wary of where data is kept."[33] Due to this trend towards data localization, the status of these clouds under the CLOUD Act becomes an especially important question. 22

22 CLOUD Act, *supra* note 1, at § 105(a) (adding 18 U.S.C. § 2523(b)(1)).

23 CLOUD Act, *supra* note 1, at § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(iv)-(v)).

24 As a result, these restrictions are less strict than analogous concepts found in the Wiretap Act, the U.S. statute that regulates the surveillance of electronic communications by U.S. law enforcement agencies within the U.S. Regarding "targeting," the CLOUD Act forbids a foreign government from "intentionally target[ing] a United States person or a person located in the United States." *Id.* at § 105(a) (adding 18 U.S.C. § 2523(b)(4)(A)-(B)). It also requires adoption of "targeting procedures," so the foreign government can meet this requirement. As for "minimization," the CLOUD Act adopts the standard of the Foreign Information Surveillance Act (FISA), which is far more lenient than that of the Wiretap Act. Like FISA, the CLOUD defines "minimization" in data gathering procedures as subject to a mere relevancy standard. Specifically, it creates an obligation for government authorities to develop "minimization procedures" to block collection of or delete "material found not to be information that is, or is necessary to understand or assess the importance of information that is relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person." *Id.* at § 105(a) (adding 18 U.S.C. § 2523(b)(4)(G)).

25 *Id.* at § 105(a) (adding 18 U.S.C. § 2523(b)(4)(D)(vi)).

26 *Mark Scott, U.S. Tech Giants Are Investing Billions to Keep Data in Europe*, N.Y. Times (Oct. 3, 2016), https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html.

27 *Id.*

28 *See Paul M. Schwartz, Legal Access to the Global Cloud*, 118 Colum. L. Rev. 1681 (forthcoming 2018).

29 *See id.*

30 Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677, 679 (2015). For an argument that laws requiring local data localization are driven by "[n]ation-states who perceive themselves to be at a comparative disadvantage in the efficiency of their Internet signals intelligence," see *John Selby, Data Localization Laws: Trade Barriers or Legitimate Responses to Cybersecurity Risks, or Both?*, 25 Int'l J. Law & Info Tech 213, 232 (2017).

31 See § 113b subs. 1 Telekommunikationsgesetz (TKG – Telecommunications Act). The same applies for tax data according to § 146 subs. 2 Abgabenordnung (AO – Federal Tax Procedure Act)..

32 *Id.*

33 *Scott, supra* note 24.

2. Clashes Between the CLOUD Act and GDPR: Incentives for Data Localization

23 To summarize this section's conclusions, data localization clouds will receive somewhat greater protection pursuant to a comity analysis under Step One and Step Two of the CLOUD Act. At the same time, however, the resulting analysis by a U.S. court is likely to be highly fact-specific. There are also significant conflicts ahead between the CLOUD Act and EU data protection, as well as a corresponding need for a U.S.-E.U. accord.

a) Step One and the Factors for a General Comity Analysis

24 With the enactment of the CLOUD Act, Congress made explicit that the SCA's reach is international. A data localization cloud anywhere in the world is subject to it, but the cloud provider also has a right to judicial review of SCA orders. The provider can contest an SCA order in U.S. court, which will then apply a common law comity analysis. In this decentralized process, only one thing is certain: some foreign providers are likely to win these comity cases, and others are likely to lose.

25 A comity analysis becomes necessary when there is a conflict of laws between an SCA order and EU data protection law. Such a conflict does exist between Article 48, GDPR, and the CLOUD Act. Indeed, EU experts have already expressed doubts about whether the CLOUD Act meets the standards of Article 48, GDPR. For example, *Axel Spies* predicts a "collision course" as set between the CLOUD Act and Article 48, GDPR.[34]

aa) Conflict With GDPR Requirements

26 The collision follows from Article 48's permitting data transfers for court orders under only restricted conditions. That part of the GDPR generally permits international transfers of personal data to comply with a "judgment of a court or tribunal ... of a third country" that requires such a disclosure. But such an order is only valid "if based on an international agreement, such as a mutual legal assistance treaty."[35] Such a valid agreement can be between a third country, such as the U.S., and either the Union or a Member State. The analysis here is straightforward: the CLOUD Act is not an "international agreement" in the sense of Article 48. It is a domestic law that one country, the U. S., enacted. Hence, a request for information to a European cloud provider pursuant to the SCA places that provider in conflict with local law. Indeed, Recital 115, GDPR, explicitly warns against reliance on the "judgments of courts" that are "not based on an international agreement." This Recital also states, "The extraterritorial application of those laws, regulations and other legal acts may ... impede the attainment of the protection of natural persons ensured in the Union by this Regulation."[36] It should be added that the Privacy Shield does *not* provide a basis for such a transfer. While the Privacy Shield permits transfers to U.S. companies that have entered into it, U.S. law enforcement authorities are not Privacy Shield entities.

27 More limited help may come from GDPR, Article 49 in terms of providing a path for U.S. courts or U.S. authorities with access to data. Article 49 permits a transfer of data when "necessary for the establishment, exercise or defense of legal claims."[37] It also permits a transfer "necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject."[38] In its amicus brief before the U.S. Supreme Court in *Microsoft Ireland*, the European Commission observed that the GDPR made MLAT's "the preferred option for transfers."[39] At the same time, however, it conceded that GDPR, Article 49, albeit to be interpreted strictly, was relevant concerning a transfer of personal data from the EU to a third country. Regarding the "public interest" grounds of Article 49, the Commission noted that Article 83, Treaty on the Functioning of the European Union, had identified "several areas of crime that are particularly serious and have cross-border dimensions, such as illicit drug trafficking."[40] As to the "legitimate interests" of the controller, the Commission noted the need here for scrutiny of factors such as procedural guarantees under which the foreign court order was adopted and "applicable data protection rules in place in the third country."[41] Just as critically, the brief of the Commission noted that such transfers pursuant to Article 49 would be permissible only if not ongoing, and concerning only a limited number of data subjects.

28 Thus, GDPR, Article 49 does not offer a miraculous fix, or magic wand, for the complex issue of U.S. court orders seeking access to cloud information. A cloud provider in the E.U. is still likely to face circumstances where it will be obligated to make a motion before a U.S. court to quash a transfer seek the protection of the CLOUD Act's general comity clause. In this scenario, an SCA order would require disclosure, and EU data protection law would forbid it.

bb) Key Factors of a Comity Analysis

29 Comity analysis is designed for just this kind of situation; it rests on the need, whenever possible, to "reconcile[] the central concerns" of domestic and foreign laws when they conflict.[42] In acting to respect comity, courts protect "the mutual interests of all nationals in a smoothly functioning international legal regime."[43] As the Supreme Court already recognized at the end of the Nineteenth Century, comity involves "the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights

34 *Axel Spies, USA: Gesetzgeber billigt Datenzugriff außerhalb der USA (CLOUD Act)*, ZD Fokus V-VI, Zeitschrift für Datenschutz (5/2018).

35 GDPR, *supra* note 2, at Art. 48.

36 GDPR, *supra* note 2, at Recital 115.

37 GDPR, *supra* note 2, at Art. 49(1)(e).

38 GDPR, *supra* note 2, at Art. 49(1).

39 Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, Microsoft Ireland, No. 17-2 14 (Dec. 13, 2017).

40 Id. at 15.

41 Id.

42 Société Nationale Aérospatiale v. U.S. Dist. Court for S. Dist. Of Iowa, 482 U.S. 522, 555 (1987).

43 *Id.* It is a concept of "judicial self-restraint in furtherance of policy considerations which transcend individual lawsuits." Volkswagenwerk Aktiengesellschaft v. Superior Court, 176 Cal. Rptr. 874, 884 (Ct. App. 1981).

of its own citizens, or to other persons who are under the protection of its laws."[44]

30 The CLOUD Act itself only generally provides for a "comity analysis" and references "common law standards," without more explicit language. As for these common law standards, the Restatement (Third) of Foreign Relations contains the most influential expression in the U.S. of these rules. It contains a five-part benchmark; according to the Restatement (Third), judges are to evaluate: "[1] the importance to the investigation or litigation of the documents or other information requested; [2] the degree of specificity of the request; [3] whether the information originated in the United States; [4] the availability of alternative means of securing the information; and [5] the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located."[45] Some U.S. courts have expanded the required analysis in their jurisdiction by tacking on additional factors.[46]

31 A comity analysis grants some additional protection to cloud data that is stored with an EU-localized cloud provider, as opposed to a U.S.-based cloud provider. This result follows from two of the five Restatement Factors. One element, the third Restatement factor, in the required comity analysis concerns "whether the information originated in the United States." There is some potential ambiguity here as to whether this language refers to where the information is *stored* or where it is *accessed*. For a localized cloud, information stored in the EU referring to a non-U.S. person would benefit from being both *stored* outside of the U.S. and *accessed* outside of the U.S. This distinction becomes meaningful with regard to the use of a data shard cloud, such as Google provides. In that type of cloud, data is dynamically distributed among different data centers. In the Google cloud, the company can only retrieve the information from within the U.S., even if the data is also stored extraterritorially.[47] A data shard cloud keeps information ceaselessly in motion among data centers throughout the world. In contrast, an EU-localized cloud would receive greater protection under a comity analysis than information stored with a data shard cloud or information stored with a U.S.-based cloud provider and accessed by the provider within the U.S.

32 Another Restatement element, its fifth factor, looks to "the extent to which ... compliance with the request would undermine important interests of the state where the information is located." Here, too, a localized cloud provider in the EU can expect that this factor would weigh in its favor under a comity analysis. The European rights regime includes both privacy and an explicit right to data protection. Both interests now have the status of a fundamental right in Europe. Within the European Union, the key constitutional document is the Charter of Fundamental Rights.[48] With the signing of the Lisbon Treaty by EU Member States, the Charter became binding constitutional law for the EU in 2009.[49] The Charter protects privacy and also contains an explicit right to data protection.[50] Beyond the EU, many European countries, including Germany, have further obliged themselves to protect privacy and data protection pursuant to the European Convention of Human Rights. Where the Charter of Fundamental Rights is a key constitutional document of the EU, the European Convention of Human Rights is an international treaty open to countries beyond the Member States of the EU.[51] The Convention is also part of the EU legal system pursuant to the Treaty of the European Union.[52] It explicitly protects "a right to respect for ... private and family life." The European Court of Human Rights has drawn on Article 8 to identify specific rights regarding data protection.[53] In sum, data protection is a core part of a legal culture of fundamental rights in Europe.

cc) The Resulting Fact-Specific Evaluation

33 While a localized cloud is likely to receive additional protection under the CLOUD Act, a comity analysis will look to the specific circumstances of the case at hand. The Restatement requires such a targeted analysis. Its first factor calls for a court to assess "the importance to the investigation or litigation of the documents or other information requested." Moreover, the fifth factor considers whether "noncompliance with the request would undermine important interests of the United States." As the Congressional Research Service notes, a comity analysis "is likely to be a highly fact-specific evaluation that depends on the specific circumstances of a demand for data stored overseas."[54]

34 In short, the CLOUD Act does not resolve all legal issues about the use of the SCA to gather data from extraterritorial clouds. For clouds outside the U.S., the CLOUD Act creates a decentralized approach to contested data access requests under which U.S. courts will apply a comity analysis. For non-U.S. customers, there will be benefits to using such clouds located or accessible only outside the U.S., as that will increase their protection under certain comity factors.

b) Step Two and the Factors for Specific Comity Analysis

35 What happens to non-U.S. localized clouds once the CLOUD Act's second phase takes effect? As noted, this part of the law requires the enactment of an executive agreement between the U.S. and a foreign government. Once such an agreement is in place, each government will receive direct access to cloud pro-

44 Hilton v. Guyot, 159 U.S. 113, 164 (1895).

45 *Id.*

46 Richmark Corp v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (adding the following two factors: [1] "the extent and the nature of the hardship that inconsistent enforcement would impose upon the person," and [2] "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.").

47 For a complete discussion of the three main models of cloud computing and their legal implications, see *Schwartz, supra* note 26, at 1708-1735.

48 Charter of Fundamental Rights of the European Union, 2000 O.J C 364/10.

49 *Jean-Claude Piris*, The Lisbon Treaty 146 (2010).

50 *Paul M. Schwartz & Karl-Nikolaus Peifer, Transatlantic Data Privacy*, 106 Geo L. J. 115, 125–126 (2017).

51 Convention for the Protection of Human Rights and Fundamental Freedoms, art. 1, Nov. 4, 1950, 213 U.N.T.S. 222.

52 Treaty of the European Union, Art 6(2).

53 *Orly Lynsky*, The Foundations of EU Data Protection Law 106-112 (2015).

54 *Stephen P. Mulligan*, Cong. Research Serv., Cross-Border Data Sharing Under the CLOUD Act 10 (2018), https://fas.org/sgp/crs/misc/R45173.pdf.

viders in the other country, if it complies with applicable domestic procedures for surveillance orders.

36 Moreover, as is the case for SCA warrants under *Step One*, cloud providers will have the ability to contest these data requests in U.S. courts. To do so under *Step Two*, however, the cloud provider must reasonably believe that "the customer or subscriber is not a United States person and does not reside in the United States," and the U.S. court must find that these conditions are met. As a result, the EU cloud provider now has a powerful incentive to document the nationality of its customers.[55] This part of the CLOUD Act also does more than reference general comity principles; it lists specific factors that the U.S. court is to apply in its analysis. The ultimate test is "that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government."

37 In contrast to the five factors of the Restatement's comity analysis, the CLOUD Act lists eight factors for its specific comity analysis. While the eight factors largely track those of the Restatement, the additional factors touch on requests by foreign governments to U.S. providers.[56] From the viewpoint of a cloud provider with a data center localized outside of the U.S., the CLOUD Act's first four factors are key. These look at:

38 [1] the interests of the qualifying foreign government in preventing any prohibited disclosure; [2] the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; [3] the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States ...; and [4] the nature and extent of the provider's ties to and presence in the United States ... .[57]

39 Some of these factors are similar to those under the CLOUD Act's general comity analysis for its extension of the SCA, and some are different.

40 A factor similar to one in the general comity analysis looks to "the nature and the extent of the provider's ties to and presence in the United States." This factor weighs in favor of a localized EU data provider. Such a provider has established a cloud that is located outside of the U.S. Another of Step Two's comity factors calls for evaluation of the interest of the foreign government. As under the general comity analysis, the strong EU interest in data protection as a constitutional right will weigh in favor of the localized cloud provider in the EU.

aa) A Future Sanctions Arms Race?

41 A new comity factor in this part of the law calls for consideration of the "likelihood, extent, and nature of penalties" for a provider due to a conflict of laws. Here, the strong penalties in the GDPR become relevant. Already, academics in the United Kingdom have warned of "a sanctions arms race" between legal systems that regulate the cloud.[58] As W. Kuan Hon and his co-authors state, "When different states claim jurisdiction over the same organization and, more specifically, its data processing, and complying with one state's demands would break the laws of another state, the organization is in the invidious position of having to decide which state's laws to break."[59] Hon and his co-authors predict that organizations, in deciding which state's laws to obey and which to break, will consider "the nature and severity of sanctions involved."[60]

42 In such an arms race, the EU has strong weapons available to it. One of the most important changes in the GDPR is to greatly increase the available fines for violation of data protection law. The GDPR permits fines to reach up to 20 million Euros, or up to 4 % of "the total worldwide annual turnover of the preceding financial year, whichever is higher."[61] It also requires penalties to "be effective, proportionate, and dissuasive."[62] The GDPR squarely places "the transfers of personal data to a recipient in a third country" under this provision for high penalties.[63] Pursuant to the GDPR, Germany has recently enacted a new version of its Federal Data Protection Law (BDSG-New), and this statute follows the GDPR's scheme for fines. The BDSG-New authorizes greatly increased fines.[64] These are as much as sixty-six times higher than were permitted under the previous BDSG. Overall, as a treatise on the GDPR observes, this new order ensures that "appropriate, hard, and dissuasive sanctions" are in place for violations of data protection law.[65]

43 As noted above, however, the necessary comity analysis under an executive order is likely to be fact-specific. For example, one factor in this part of the CLOUD Act calls for assessment of the importance of the sought-after information to the investigation, as well as the "interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure."[66] A court may well order compliance for a localized cloud under a bilateral executive agreement if timely and effective access to the information bears on a matter of great significance for a significant criminal investigation in the U.S.[67]

---

55 Other areas of law have developed such "know your customer" requirements. A classic area with similar required documentation is the financial service sector. *Daniel Solove & Paul M. Schwartz*, Privacy Law Fundamentals 146-47 (2017).

56 These additional factors are: "[5] the nature and extent of the provider's ties to and presence in the United States; [6] the importance to the investigation of the information required to be disclosed; [7] the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and [8] if the legal process has been sought on behalf of a foreign authority ..., the investigative interests of the foreign authority making the request for assistance." CLOUD Act, *supra* note 1, at § 103(b) (adding 18 U.S.C. §§ 2713(h)(3)(A)-(H)).

57 *Id.*

58 *W. Kuan Hon* et al., *Policy, Legal and Regulatory Implications of a Europe-Only Cloud*, 24 Int'l J. Law & Information Tech. 251, 276 (2016).

59 *Id.*

60 *Id.*

61 GDPR, *supra* note 2, at Art. 83(4).

62 *Id.* at Art. 84(1).

63 *Id* at Art. 83(5)(c). *See Paul M. Schwartz, The EU-U.S. Privacy Collision*, 126 Harv. L. Rev. 1966, 1997 (2013).

64 BDSG-New, Sec. 83, Section 84.

65 *Jan Phillip Albrecht & Florian Jotzo*, Das neue Datenschutzrecht der EU Par. 1, p. 121 (2017).

66 CLOUD Act, *supra* note 1, at § 103(b) (adding 18 U.S.C. § 2713(h)(3)(A)).

67 *Id.* at § 103(b) (adding 18 U.S.C. § 2713(h)(3)(G)).

44 The record is already a mixed one when U.S. courts apply comity analysis to contested discovery requests in the context of civil litigation. Numerous cases have seen EU defendants objecting to discovery requests from U.S. litigants and claiming their compliance would violate EU data protection law. Some U.S. courts have been sympathetic to the high value of data protection law in the EU legal order, others have not.[68] In the relevant academic literature in the U.S., recent pleas have been made for greater attention to the importance of EU law in comity analysis. As a general matter, Diego Zambrano has pointed to the Supreme Court's recent *Daimler* decision and other case law as demonstrating that international comity is a "critical concern" and not "a formality."[69] There is a need, above all, for a "serious and rigorous consideration of foreign countries' interests."[70] Zambrano views comity as especially important in today's intertwined global economy.[71] More specifically, Samantha Cutler argues for U.S. courts with comity cases to recognize the great significance of data protection within the EU.[72] She writes, "In order to duly respect EU data privacy law, U.S. courts must be willing to consider how important the right to privacy is in the European Union and the fact that litigants face an increased risk of sanctions for data privacy violations." Cutler observes, "The evolution of EU data privacy law over the last two decades shows an increasing trend towards stronger protections for data privacy and greater obligations and liability for data controllers."[73]

bb) Threshold Requirement: An "International Agreement"

45 There is a final potential twist here. The CLOUD Act does not qualify as "an international agreement" under Article 48, GDPR. In contrast, an executive agreement between a third country, such as the U.S. and a Member State, will meet this requirement. At the same time, however, there is an open question about whether such agreements meet the overall constitutional standard in EU law for adequacy.[74]

46 In its *Schrems* decision, the CJEU makes clear that adequacy requires that protections be "essentially equivalent."[75] As *Christopher Kuner* observes, this opinion connects the requirement of an adequate level of protection "to the level of data protection required by the Charter."[76] *Kuner* adds, "By defining the standard that third countries must meet to be declared 'adequate' as that of essential equivalence with EU law, the CJEU has set the global data protection bar at a high level."[77] Just as it decided on the fate of the Safe Harbor agreement, the CJEU will have the ultimate word about the sufficiency of any executive agreements developed under the CLOUD Act.

IV. The Need for EU and U.S. Cooperation

47 This Article has identified potential collisions ahead between the EU and the U.S. following enactment of the CLOUD Act. Because the CLOUD Act itself does not qualify as an Article 48, GDPR "international agreement," there is a conflict between SCA orders to EU cloud providers and EU data protection law. In addition, executive agreements created under the CLOUD Act's Step Two may fail to provide "adequate" protection.

1. EU-U.S. Data Protection Umbrella Agreement

48 These developments show U.S. and EU law moving in different directions and headed for future clashes. Yet, there is also a major area of transatlantic convergence. The EU and U.S. share a commitment to combatting international terrorism and organized criminality. Both political systems are already collaborating in this area. Results of the existing transatlantic cooperation include the EU-U.S. data protection "Umbrella Agreement" of June 2016.[78] This agreement permits information sharing "to combat crime, including terrorism."[79] The Umbrella Agreement also establishes data privacy protections for all personal information that is shared pursuant to it. As this new accord demonstrates, the United States, the Commission of the EU, and EU Member States all share an interest in establishing a legal framework for the exchange of information "to prevent, investigate, detect and prosecute criminal offences, including terrorism."[80]

2. EU Measures Similar to the CLOUD Act

49 The EU is also working on putting in place the elements of its own internal EU equivalent to the CLOUD Act. These are its Law Enforcement Directive and its Proposed Regulation for a European Production Order[81] and a European Preservation Order.[82]

50 First, the Law Enforcement Directive creates a new framework for data processing activities performed by law enforcement authorities. Like any EU directive, it is not directly binding but requires Member States to enact national laws that will reflects its principles, including that of strong protection for personal

68 See generally *Daniel J. Solove & Paul M. Schwartz*, Information Privacy Law 1174-75 (6th ed. 2018).

69 *Diego Zambrano*, *A Comity of Errors*, 34 Berk. J. Int'l Law 157, 184 (2016).

70 *Id.* at 199.

71 *Id.* at 198-97.

72 Samantha Cutler, *The Face-Off Between Data Privacy and Discovery*, 59 B.C. L. Rev. 1513, 1532 (2018).

73 *Id.* at 1534.

74 *Cording/Götzinger*, CR 2018, 636 Rz. 24 (citing CJEU, Opinion 1/15 of 26 July 2017 on the draft Agreement between Canada and the EU regarding Transfer of Passenger Name Record Data from the EU to Canada; *Sydow* in Kühling/Buchner, 2. Aufl. 2018, Art. 48 DSGVO Rz. 16.

75 Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (Oct. 6, 2015).

76 *Christopher Kuner, Reality and Illusion in EU Data Transfer Regulation Post* Schrems, 18 German L.J. 881, 893 (2017).

77 *Id.*

78 Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, E.U.-U.S., June 2, 2016, T.I.A.S. No. 17-201, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (entered into force Feb. 1, 2017) ("Umbrella Agreement").

79 *Id.*

80 *See id.*

81 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, O.J. EU L 119/89 (4.5.2016)[hereinafter Law Enforcement Directive].

82 European Comm'n, Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (2018)[hereinafter Production Order Proposal].

data. Once the law within the EU is harmonized, there is to be a few flow of information among law enforcement authorities "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties."[83] The Law Enforcement Directive permits a transfer to a "third country," that is, a nation that does not belong to the EU on the basis of an adequacy decision, or if it is subject to "appropriate safeguards" that are "provided for in a legally binding instrument."[84] In its Article 38, the Law Enforcement Directive allows a derogation in an individual case for defense of legal claims, but only if a "transferring competent authority determines that fundamental rights and freedoms of the data subject" are *not* greater than the public interest in the information.[85]

51 Second, on April 17, 2018, the Commission introduced a draft Production and Preservation Regulation. Under this proposed Regulation, a new kind of Europe-standard order, to be issued by a judicial authority in a Member State, would seek production or preservation of data stored by a cloud provider located in another EU jurisdiction. Unlike the CLOUD Act, however, the proposed orders would not permit surveillance of real time data, but only the production and preservation of stored data.[86] In a related policy initiative, a proposed Directive,[87] the EU would require online cloud providers, including overseas ones, to appoint a legal representative in the EU. This individual would be available to be served with papers in criminal and terrorism investigations in the EU and to be a point person for access to data stored outside the EU. As the Commission explains, the resulting "harmonised approach" creates "a level playing field for all companies offering the same type of services in the EU, regardless of where they are established or act from..."[88] These rules will not only "eliminate obstacles to the provision of services," but ensure both "a better functioning of the internal market [and] a more coherent approach to criminal law in the Union."[89]

3. A Critical Balancing Act

52 These policy initiatives indicate a common meeting ground for the U.S. and EU regarding the regulation of access to cloud data. The great need is for the EU and U.S. to find a way to protect data privacy, while also safeguarding the ability of law enforcement to investigate and prosecute crime. From the EU perspective, it is clear that the CLOUD Act cannot by itself justify access to data localized in the U.S., and this murky situation cannot simply be resolved through bilateral executive agreements as the U.S. statute foresees. Thus, EU justice commissioner *Vera Jourova* has criticized the enactment of the CLOUD Act "in a fast-track procedure" and complained that this unilateral action "narrows the room for the potential compatible solution between the EU and the U.S."[90]

53 Although the U.S. and Great Britain are now preparing the first executive agreement, Jourova has indicated her wish for "a unified, harmonized approach" for the rest of Europe. In place of accords between the U.S. and individual EU states, the EU wishes to establish a U.S.-EU agreement that provides a counterpart to its "European Production and Preservations Orders." From the viewpoint of the Commission, then, the difficulty may be less the content of the CLOUD Act than the potential that the U.S. might act unilaterally to enter nation-by-nation agreements, as opposed to a wholesale agreement with the EU.

In short, this area is one of legal uncertainty until a U.S.-EU 54
accord is in place. Until that agreement is reached, however, all clouds will not be created equal for European customers. Data localization clouds in Europe will provide additional legal protections against U.S. law enforcement data requests. The key factors will concern data residency in Europe and cloud providers who can only access their data centers from within Europe. At the same time, however, a U.S. court will look to the specific factors involving a contested data transfer.

V. Conclusion

The CLOUD Act sets into motion two major changes to U.S. 55
surveillance law. It extends the reach of SCA warrants extraterritorially, requiring cloud providers to comply with warrants regardless of where the requested data is located. And it sets forth a process for establishing bilateral accords under which the U.S. and qualifying foreign governments can grant each other reciprocal authority to request data directly from the cloud providers in each other's jurisdictions. Both mechanisms embrace a global interoperable Internet and the fundamental idea of reciprocity in international data transfers. If a conflict of laws then occurs between legal systems, the courts in each country engage in a comity analysis, taking into account the interests of each nation.

Putting the CLOUD Act into practice will not be simple, how- 56
ever, in large part because the U.S. and the EU have different approaches to data privacy. Due to the GDPR, the CLOUD Act may not succeed in its attempt to extend the reach of SCA warrants to EU Member States. The CLOUD Act may well conflict with the GDPR and EU data protection law. At present, the enforcement of an SCA warrant under the CLOUD Act will ultimately depend on a multi-factored comity analysis performed by individual courts.

When faced with legal uncertainty, cloud providers can and 57
will shift to localized cloud models that shelter data beyond the exclusive reach of the U.S. But such technical localization fails to address the basic need for the CLOUD Act's policy purpose of data sharing between nations to combat serious crime and terrorism. This Article proposes that the most sensible and efficient path to legal certainty for cloud providers would be an accord between the U.S. and the EU itself. Such a harmonized approach would reflect the CLOUD Act's embracement of reciprocity and also align privacy laws with the technical reality of an ever-connected world of cloud computing.

---

83 Law Enforcement Directive, supra note 81, at Recital 4.

84 Id. at Art. 36, Art. 38.

85 Id. at Art. 38.

86 Production Order Proposal, supra note 80, at 5.

87 European Comm'n, Proposal for a Directive Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings (2018).

88 *Id.* at 3.

89 *Id.*

90 *Nikkolaj Nielsen, Rushed US Cloud Act Triggers EU Backlash*, eu observer (Mar. 26, 2018), https://euobserver.com/justice/141446.

Prof. Paul Schwartz

Jefferson E. Peyser Professor at Berkeley Law School and a Director of the Berkeley Center for Law and Technology as well as Special Advisor at Paul Hastings, a global law firm, in the Privacy and Data Security Practice.

He is the author of many books, including the leading casebook, Information Privacy Law, and the distilled guide, Privacy Law Fundamentals, each with Daniel Solove.

www.paulschwartz.net

Prof. Dr. Karl-Nikolaus Peifer

Professor of Law at the University of Cologne, Director of the Institute for Media and Communications Law and Judge at the Regional Court of Appeals in Cologne.

Research focus on Intellectual Property and Media Law including Data Protection Regulation.

Web-address: institut-medienrecht.de or media-law.cologne.