4 | 2019
20th Year
15 August 2019
P. 97–128

CRi

Computer Law Review International

A Journal of Information Law and Technology

cr-international.com

ottoschmidt

86203501904

Alexander A. Berengaut / Lars Lensdorf

The CLOUD Act at Home and Abroad

Addressing the challenges of cross-border data access by law enforcement on either side of the Atlantic

This article provides an overview of the CLOUD Act, discusses how it has been interpreted by the DOJ, analyzes the impact of the Act on European companies, and considers the interaction between the Act and principles of European law, including the GDPR and the e-Evidence initiative.

I. Background

1 Law enforcement authorities increasingly rely on electronic data as evidence in criminal investigations.[1] At the same time, multinational technology companies that host electronic data on behalf of their customers often store that data in multiple countries.[2] Accordingly, authorities seeking data in criminal investigations may increasingly be required to issue legal process for data stored outside of their own borders. In such circumstances, legal process may create conflicting obligations for the technology company responsible for hosting the relevant data – *i.e.*, complying with the legal demand of the requesting country may violate the data privacy law of the country where the data is stored.[3] In the United States, law enforcement officials have generally relied on Mutual Legal Assistance Treaties ("MLATs") for cross-border data requests-an international process that ensures that legal demands respect principles of international law.[4] However, U.S. authorities have concluded the MLAT system is too slow and expensive, and they believe that the system has hindered criminal investigations.[5]

2 In February 2018, the United States enacted new legislation to address the issue of cross-border data requests: the Clarifying Lawful Overseas Use of Data ("CLOUD") Act.[6] The Act allows U.S. courts to issue legal process to covered service providers and compel them to disclose customer data "regardless" of where the data is stored. The Act also establishes a new mechanism for bilateral agreements on cross border data requests.[7] In April 2019, approximately one year after the CLOUD Act's passage, the U.S. Department of Justice ("DOJ") published a White Paper addressing the scope and purpose of the Act and responding to frequently asked questions about it.[8] Among other topics, the White Paper explains how the CLOUD Act addresses the potential conflicts of law that may arise when compliance with a U.S. government demand for data would force a technology company to violate the data privacy laws of the country where the data is stored.

3 One of these potential conflicts of law arises from Art. 48 of the European Union ("EU") General Data Protection Regulation ("GDPR").[9] Pursuant to Article 48, "[a]ny judgment of a court or tribunal and any decision of an administrative authority of a

1 *See* Clarifying Lawful Overseas Use of Data (CLOUD) Act, S. 2383, 115th Cong. § 2(1)-(2) (2018) (codified at 18 U.S.C. §§ 2713, 2523 (2018)).

2 *See* 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, at 2 (April 2019) [hereinafter White Paper], *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

3 *See id.*

4 *Id.* at 3.

5 S. 2383 § 2(2)
see White Paper, *supra* note 2, at 3.

6 *See generally* S. 2383.

7 18 U.S.C. § 2713.

8 *See generally* White Paper, *supra* note 2.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 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), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN (last visited July 23, 2019).

third country requiring a controller or processor to transfer or disclose personal data may only be" recognized or enforceable if the judgment or decision "is based on an international agreement," such as an MLAT.[10] The relevant international agreement must be in force between the requesting third country and the EU or a Member State, without prejudice to other grounds for transfer pursuant to Chapter 5 of the GDPR.[11]

4 Meanwhile, the EU has also undertaken to address the issue of cross-border data requests. In April 2018 the European Commission announced an e-Evidence initiative,[12] which concerns the ability of law enforcement and judicial authorities to obtain electronic evidence (or "e-Evidence"). This e-Evidence initiative specifically focuses on providing law enforcement officials in EU countries with mechanisms to compel the production or preservation of data from providers offering services in the EU, even if the provider is established, or the data in question is stored, outside the EU.[13]

5 Most recently, on June 6, 2019, the European Council adopted two mandates authorizing the European Commission to negotiate on behalf of the EU. The first mandate authorizes negotiation of an agreement with the United States facilitating access to e-evidence for the purpose of judicial cooperation in criminal matters. The second mandate authorizes participation in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention.[14]

II. Overview of The CLOUD Act

6 The CLOUD Act contains two distinct parts:

- *First*, the Act allows U.S. federal, state, and local authorities to issue legal process to covered technology service providers for data, even if the data is stored overseas.[15] More specifically, the Act authorizes such authorities to issue orders to all providers of defined technology services, so long as they are subject to U.S. jurisdiction and in "possession, custody, or control" of the data sought "regardless" of whether the data is stored inside or outside of the U.S.[16] As discussed in Section IV.2.b below, however, a provider may challenge an order for data stored outside the United States if compliance would create a conflict-of-law situation.

- *Second*, the CLOUD Act creates a new framework for countries to enter into bilateral agreements on cross-border data requests.[17] These agreements remove restrictions under each country's laws and allow technology companies to comply with qualifying, lawful orders issued directly by the other country.[18]

7 Before a country may enter into a CLOUD Act agreement, the U.S. Attorney General must submit certain written certifications to Congress regarding the foreign country.[19] Those certifications must find that the country meets specific criteria establishing that its domestic law affords robust substantive and procedural protections for privacy and civil liberties. Additionally, the foreign government must agree not to target U.S. persons, must adopt procedures to minimize the acquisition and retention of information about U.S. persons, and must not impose a decryption obligation on providers through the agreement.[20]

8 Bilateral agreements must also contain a number of limits on the types of orders that may be submitted by the foreign government directly to a U.S. provider, including: (i) orders must be for the purpose of obtaining information relating to a serious crime, including terrorism; (ii) orders must identify a specific person, account, address, device, or other identifier; (iii) orders must comply with the foreign government's domestic law; (iv) orders must be based on requirements for a reasonable justification based on articulable and credible facts; and (v) orders must be subject to judicial review prior to, or in enforcement proceedings regarding, enforcement of the order.[21]

9 These two components of the CLOUD Act were each elaborated upon by the White Paper.[22]

III. Approach of the Department of Justice White Paper

10 The White Paper begins by observing that, where laws of countries conflict, technology companies may be forced to choose which laws to follow "knowing that they may face consequences for violating another country's laws."[23] Such conflicts can pose "serious problems for governments seeking data and can frustrate important investigations."[24] Given these issues, the White Paper characterizes the CLOUD Act as "represent [ing] a new paradigm: an efficient, privacy and civil liberties-protective approach to ensure effective access to electronic data that lies beyond a requesting country's reach due to the revolution in electronic communications, recent innovations in the way global technology companies configure their systems, and the legacy of 20th century legal frameworks."[25]

11 The White Paper explains how bilateral agreements negotiated under the CLOUD Act can reduce such conflicts of laws. Such agreements would "lift any restrictions under U.S. law on companies disclosing electronic data directly to foreign authorities

10 *Id.*
11 Chapter 5 of the GDPR, which includes Article 48, concerns transfers of personal data to third countries or international organizations generally.
12 European Commission, *Internal EU Rules: Proposal on e-evidence*, E-evidence – cross-border access to electronic evidence: Improving cross-border access to electronic evidence, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en (last visited July 23, 2019).
13 *Id.*
14 *See* Press Release, European Council (June, 6, 2019), available at https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.
15 18 U.S.C. § 2713.
16 *Id.*
17 *Id.* § 2523 .
18 *Id.*
19 *Id.* § 2523(b)(1).
20 *Id.* § 2523(b)(2).
21 *Id.* § 2523(b)(3)(d).
22 Additional background on the Cloud Act is available in *Paul Schwartz* & *Karl-Nikolaus Peifer*, *Data Localization Under the Cloud Act and the GDPR*, 20 Comp. L. Rev. Int'l 1, 1–10 (2019).
23 White Paper, *supra* note 2, at 3.
24 *Id.*
25 *Id.* at 2.

for covered orders in investigations of serious crime."[26] In doing so, the agreements "would permit U.S.-based global [technology companies] to respond directly to foreign legal process in many circumstances."[27] The White Paper, in its FAQs portion, also makes clear that CLOUD Act agreements are to supplement, rather than replace, existing MLATs.[28]

12 The FAQs portion of the White Paper addresses a number of common questions about the CLOUD Act, including about the extraterritorial reach of U.S. legal process codified in the first part of the Act and the ability of providers to challenge legal demands that create conflict-of-law situations.[29] For example, the FAQs responses state that the CLOUD Act did not give U.S. courts expanded jurisdiction over non-U.S. persons. Rather, DOJ states that the Act requires companies already subject to jurisdiction in the U.S. to provide data in response to U.S. legal process, regardless of where the data is stored. The White Paper also states that if a U.S. order conflicts with foreign law, "U.S. courts can be expected to apply long-standing U.S. and international principles regarding conflicts of law to ensure appropriate respect for international comity by applying a multi-factor balancing test, taking into account the interests of both the United States and the foreign country."[30]

IV. The Impact of the CLOUD Act Outside the United States

13 As the White Paper and its accompanying FAQs reflect, the impact of the CLOUD Act outside the United States has garnered significant attention. This section analyzes three respects in which the CLOUD Act may apply outside the United States and interact with non-U.S. legal regimes: (i) the application of the CLOUD Act to non-U.S. service providers; (ii) the ability of providers covered by the CLOUD Act to challenge legal demands that create conflict-of-law situations; and (iii) the relationship between the CLOUD Act and the e-Evidence initiative under EU law.

1. Application of the CLOUD Act to Non-U.S. Service Providers

14 Legal process issued under the CLOUD Act can be enforced against any covered technology providers subject to U.S. jurisdiction that "possess, have custody or control" of the requested data regardless of where it is stored.[31] As the White Paper explains, under this standard, the CLOUD Act thus applies not only to U.S. providers, but all providers subject to personal jurisdiction in U.S. court.[32] The CLOUD Act did not alter U.S. legal principles governing jurisdiction, and the question whether providers established outside the U.S. are subject to personal jurisdiction in U.S. courts (and thus are bound by the CLOUD Act) accordingly depends on these background jurisdictional principles.

15 In short, U.S. courts recognize two types of personal jurisdiction:[33]

- *General jurisdiction*, in the corporate context, typically exists in U.S. court only if the relevant company is headquartered or incorporated in the United States.[34] If a company is found to be subject to general jurisdiction, it may face "any and all claims" even when the suit is distinct from the company's dealings in the United States.[35]
- *Specific jurisdiction*, by contrast, may exist even if a non-U.S. company is headquartered and incorporated outside the United States. Although the test for specific jurisdiction has several elements, the key question is whether the company has sufficient "*minimum contacts*" with the United States.[36] Under this doctrine, companies may face only those lawsuits that "derive[] from" or are "connected with" such contacts.[37]

16 There are many examples of foreign companies found to have sufficient "*minimum contacts*" with the United States. For example, sufficient minimum contacts were found when a German cloud provider had a "regular course of sales" in the United States.[38] The court reasoned that the company could "reasonably anticipate[]" being subject to U.S. specific jurisdiction because it obtained U.S. contracts via its website and the contracts yielded $200,000 in business.[39]

17 Even if a non-U.S. provider is found to be subject to U.S. jurisdiction, the CLOUD Act may only require the company to disclose information in its "possession, custody, or control."[40] Whether a company has the requisite possession, custody, or control of information is a highly fact-specific inquiry that generally depends on whether the company has the "legal right" or "practical ability" to access the information.[41]

2. Mechanisms to Challenge CLOUD Act Orders

18 As set out in the White Paper, one goal of the CLOUD Act is to address conflict-of-law situations, where compliance with U.S. legal process may force a provider to violate another country's data privacy law. At the same time, as set out above, the CLOUD Act also compels providers subject to U.S. jurisdiction to produce data stored outside the United States-a rule that creates potential conflict insofar as other countries regulate data

26 *Id.* at 4.
27 *Id.*
28 *Id.* at 11.
29 *See generally id.* at 10–18.
30 *Id.* at 16.
31 18 U.S.C. § 2713.
32 *See* White Paper, *supra* note 2, at 8.
33 *Goodyear Dunlop Tires Operations, S. A. v. Brown*, 564 U.S. 915, 919 (2011).
34 *Id.* at 924.
35 *Id.* at 919, 924.
36 *Int'l Shoe Co. v. Wash.*, 326 U.S. 310, 316 (1945).
37 *Goodyear*, 564 U.S. at 919.
38 *Plixer Int'l, Inc. v. Scrutinizer GmbH*, 905 F.3d 1, 10 (1st Cir. 2018).
39 *Id.*
40 18 U.S.C. § 2713 (2018).
41 The highly fact-intensive inquiry requires analysis of the specific relationship between the entity receiving legal process and the information at issue. In some cases, the "legal right" prong is most relevant. *See Gerling Int'l Ins. Co. v. Comm'r*, 839 F.2d 131, 140–41 (3d Cir. 1988) *In re Bankers Tr. Co.*, 61 F.3d 465, 469 (6th Cir. 1995) *In re Citric Acid Litig.*, 191 F.3d 1090, 1107 (9th Cir. 1999) *Searock v. Stripling*, 736 F.2d 650, 653 (11th Cir. 1985). In other cases, courts focus more on the "practical ability" test to determine whether possession, custody, or control exists. *See Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2d Cir. 2007) *SEC v. Credit Bancorp Ltd.*, 194 F.R.D. 469, 471 (S.D.N.Y. 2000).

stored within their borders or involving their nationals. In particular, countries may regulate disclosures of customer data stored within their countries in response to legal demands from foreign authorities.

a) Possibility for Conflict with the GDPR

19 Article 48 of the GDPR, for example, provides that subject to certain exceptions, personal data may be transferred or disclosed only pursuant to an international agreement, such as an MLAT, which is in force between the requesting third country and the EU or a Member State. Article 48 GDPR refers to conventions which explicitly cover the transfer of personal data, but not to other non-binding international conventions, recommendations or an unilateral legal demand issued by a foreign country. The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters of 18.3.1970 is currently one of the applicable treaties, although it does not apply in criminal investigations.[42] However, as Article 48 GDPR only mentions MLATs as an example, other agreements, such as the agreement concerning the transfer of flight data from the EU to U.S. authorities, may also permit the transfer of data, provided that the agreements lay down precise requirements for the specific transfer and do not undermine the level of protection afforded by the fundamental freedoms.[43] For the transfer of personal data from the EU to the United States between authorities, the EU-U.S. Data Protection "Umbrella Agreement,"[44] which was concluded between the EU and the United States in September 2015 after years of negotiations, also contains further provisions on data protection. However, this agreement does not itself provide authorization to transfer data; instead, it establishes a framework for the protection of personal data when transferred (on some other legal basis) between the EU and the United States.[45] The EU-U.S. Privacy Shield Agreement provides an additional lawful basis for transfers of data from the EU to the United States for commercial purposes, but it is unclear whether a transfer between EU and U.S. authorities pursuant to U.S. legal process would fall within scope of the EU-U.S. Privacy Shield.[46]

20 The CLOUD Act seeks to reconcile this potential for conflict by affording providers the opportunity to challenge U.S. orders if they "conflict ... with a foreign country's law forbidding production of data."[47] As the White Paper notes, if a particular order is challenged, the U.S. government could "pursue alternate channels, such as narrowing or modifying a request," resolve the conflict through "good faith negotiation," or make the request via an MLAT.[48] If the U.S. government elects to seek enforcement of the order despite the conflicting foreign law, the White Paper acknowledges that U.S. courts "can be expected to apply longstanding U.S. and international principles regarding conflicts of law to ensure appropriate respect for international comity by applying a multi-factor balancing test, taking into account the interests of both the United States and the foreign country."[49]

b) Honoring Principles of International Comity

21 This multi-factor balancing test, aimed at ensuring respect for principles of international comity, applies under the CLOUD Act in two different ways:

- *With bilateral agreement:* Where a bilateral agreement is in place, a provider seeking to challenge an order may file a motion to modify or quash the legal process under specified procedures detailed in the Act.[50] The Act also includes factors to guide the court's consideration, including the government's "investigative interest," "the interests of the qualifying government," and the "likelihood, extent, and nature of penalties" to the company at issue under the inconsistent legal requirements. With regard to orders that may be in conflict with the GDPR, pursuant to GDPR Art. 83 para. 5 lit. c, the data protection authorities may impose significant penalties.[51] Penalties may be as high as € 20 million, or four percent of the total worldwide annual turnover of the previous business year of the company (depending on which amount is higher), in the case of a violation of Art. 48 GDPR.[52] Other factors relevant to the balancing test include the nature and extent of the customer's connection to the United States, the nature and extent of the company's connection to the United States, the "importance to the investigation" of the information sought, and the "likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences."[53]

- *Without bilateral agreement:* The second application of the comity analysis occurs when a provider challenges a CLOUD Act warrant issued in the absence of a bilateral agreement. In this circumstance, common law standards (*i.e.*, not set out in the statute) would guide the inquiry.[54] Although the considerations would derive from a different source (*i.e.*, the common law), the actual factors applied in the analysis would be similar to the statutory factors discussed above. Specifically, the common law factors include, *inter alia*, the importance to the investigation or litigation of the documents or information requested, the degree of specificity of the request, whether the information originated in the United States, the availability of alternative means of securing the information, the extent to which noncompliance with the request would undermine important interests of the United States, and the extent to which compliance with the request would undermine important interests of the state where the information is located.[55]

42 *Kühling/Buchner/Schröder*, GDPR, Art. 48 marginal 16.

43 *Id.*

44 *See also* European Commission – Fact Sheet – Questions and Answers on the EU-U.S. Data Protection, Umbrella Agreement, available at http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm (last visited July 23, 2019).

45 *See* Umbrella Agreement, art. 1(3) ("This Agreement in and of itself shall not be the legal basis for any transfers of personal information. A legal basis for such transfers shall always be required.").

46 *See* Privacy Shield Overview, available at https://www.privacyshield.gov/Program-Overview (last visited July 23, 2019).

47 *See* S. 2383 § 3(c)
White Paper, *supra* note 2, at 15–16.

48 White Paper, *supra* note 2, at 15.

49 *Id.* at 16.

50 18 U.S.C. § 2703(h)(2)(A)(i) (2018).

51 Article 83 concerns general conditions for imposing administrative fines.

52 *Id.*

53 18 U.S.C. § 2703(h)(3)(A)-(H) (providing a full list of relevant considerations).

54 *Id.* § 2703 note (2018) (Rule of Construction).

55 *See* Restatement (Third) of Foreign Relations Law § 442.

22 Under either standard (*i.e.*, statutory or common law), after assessing the comity factors, the court would determine whether the provider must comply with the U.S. legal demand, despite any conflict with foreign law. Historically such challenges have been uncommon and rarely successful; nonetheless, they may become more frequent to the extent law enforcement agencies issue a greater number of extraterritorial warrants after passage of the CLOUD Act.

3. Pending European Union Initiatives Regarding Cross Border Data Requests

23 The EU has simultaneously proposed new initiatives to govern cross-border data requests that relate to the CLOUD Act. The initiatives respond to issues of resource allocation, efficiency, and transparency that the EU has identified in connection with cross-border data requests.[56] As is the case with the CLOUD Act, the proposed EU initiatives implicate conflict-of-law issues that the United States and EU are seeking to navigate. Below is a discussion of the proposed initiatives, mechanisms for challenging orders under the initiatives, and proposals for addressing conflicts with U.S. law.

a) EU e-Evidence Initiative

24 In April of 2018, the European Commission published an e-Evidence initiative, aimed at creating a new framework for EU Member States to access data across national borders.[57] Like the CLOUD Act, the initiative is designed to "make it easier and faster for ... authorities to access the electronic evidence they need in investigations to catch and convict criminals and terrorists."[58] The initiative proposes two new pieces of legislation: a Directive and a Regulation.[59] In a nutshell, these pieces of legislation would (i) require covered service providers to appoint a representative to receive and respond to data requests in criminal investigations from law enforcement authorities in any EU Member State, and (ii) create two new mechanisms for EU authorities to demand the production and preservation of data on a cross-border basis.

- *Draft Directive:* The Draft Directive would require that all covered service providers maintain a legal representative in the EU.[60] The appointed legal representative "should be able to comply with decisions and orders addressed to them by Member States' authorities on behalf of the service provider."[61] For the purposes of the Draft Directive, a company is a covered provider if it has a substantial connection with an EU Member State. A company has a substantial connection if it is "established" in an EU Member State.[62] Even if a provider is *not* established in a Member State, it will still have a substantial connection if it has a significant number of users or if it targets its activities towards a Member State.[63] Failure to comply with the Draft Directive may result in sanctions.[64]

- *Draft Regulation:* The Draft Regulation would create two new mechanisms for law enforcement to seek data on a cross-border basis: The first is the European Production Order ("EPO"), and the second is the European Preservation Order ("EPrO").[65] Both mechanisms may be issued directly to covered electronic service providers, which include "providers of electronic communications services, providers of information society services for which the storage of data is a defining component of the service provided to the user, including social networks to the extent they do not qualify as electronic communications services, online marketplaces facilitating transactions between their users ... and other hosting service providers, and providers of internet domain name and numbering services."[66] Pursuant to either type of order, EU Member State authorities may be able to compel the preservation or production, on a cross-border basis, of four data types: (i) content data, (ii) transactional data, (iii) subscriber data, and (iv) access data. Notably, EPOs and EPrOs would only apply to stored data, and they would not be available to intercept real-time communications.

- European Production Orders: EPOs permit authorities to compel covered companies that are established or represented in a second Member State to disclose data without the necessity of obtaining a further order from authorities in that second Member State.[67] Once served, providers must respond within ten days.[68] In emergency cases "where there is an imminent threat to life or physical integrity of a person or to a critical infrastructure," providers must respond within six hours.[69] Authorities can use EPOs to compel disclosure of four types of data, with the standard for the EPO varying depending on the type of data.[70] EPOs seeking subscriber or access data may be issued based on any criminal offense.[71] However, EPOs can only compel transactional or content data when the EPO is

56 *See* Explanatory Memorandum: Recommendation for a Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, at 2, COM (2019) 69, 70 final (May 2, 2018).

57 *See* Explanatory Memorandum: Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM (2018) 226 final (Apr. 17, 2018) [hereinafter Directive Memorandum]
Explanatory Memorandum: Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018) 225 final (Apr. 17, 2018) [hereinafter Regulation Memorandum].

58 *Id.*

59 *See* Directive Memorandum, *supra* note 57
Regulation Memorandum, *supra* note 57.

60 Directive Memorandum, *supra* note 57, at 4.

61 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, art. 18 COM (2018) 226 final (Apr. 17, 2018) [hereinafter Directive].

62 *Id.* at 8–9.

63 *Id.* at 9. Whether a company targets an EU Member State is a fact specific determination. *Id.* However, a substantial connection is assumed if a company directs its activities towards a member state as set out in Council Regulation No. 1215/2012, art. 17(1)(c), 2012 O.J. (L 351) 1. *Id.*

64 *Id.* art. 20.

65 Regulation Memorandum, *supra* note 57, at 4.

66 *Id.* at 4, 13.

67 *Id.* at 4.

68 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, art. 40 COM (2018) 225 final (Apr. 17, 2018) [hereinafter Regulation]. The Regulation notes that authorities retain the ability to set a deadline shorter than ten days even in non-emergency scenarios. *Id.*

69 *Id.* at 19.

70 *Id.* at 16.

71 *Id.*

based on a "serious crime"-*i.e.*, generally those punishable with at least a three-year maximum sentence.[72]

– Preservation Orders: Authorities may also use EPrOs to directly compel a provider established or represented in a second Member State to preserve data (*i.e.*, to prevent its deletion), regardless of where the data is stored. Authorities may issue an EPrO for any of the four data types mentioned above and for all criminal offenses. EPrOs "should only be made or maintained as long as necessary to enable a subsequent" production request.[73]

b) Mechanisms to Challenge Orders

25 Service providers that receive EPOs may challenge them pursuant to several different mechanisms. Providers may challenge an order as "incomplete," "manifestly incorrect," or without "sufficient information."[74] They may also challenge an order if they believe complying "manifestly violates the Charter of Fundamental Rights of the European Union or is manifestly abusive."[75] In addition, companies may challenge an order if providing the data meets a "de facto impossibility" standard.[76] A "de facto impossibility" may occur if the individual was never a customer of the provider, or if the data has been "lawfully deleted" before the order was issued.[77]

26 Moreover, similar to the CLOUD Act, the Regulation also requires Member States to provide a mechanism that would permit providers to challenge an EPO where compliance with the order would conflict with the law of a third country. A provider may challenge an order if it reasonably believes that disclosure would violate a third country's laws protecting "fundamental rights of the individual" or "fundamental interests ... related to national security or defence."[78] If such a challenge is made, a court in the issuing Member State conducts a fact specific analysis to assess whether a conflicting law exists and whether it applies in that scenario.[79] If the court finds that a conflict exists, the issuing country must notify the relevant third country.[80] If the third country objects to the order, the order would be withdrawn.[81] Alternatively, if an order is challenged by reference to a third country's conflicting law, and the law does *not* protect the "fundamental interests of the individual" or "fundamental interests ... related to national security or defence," the issuing court is under no obligation to contact authorities of the third country, but must conduct its own balancing test to determine whether to enforce the order.[82]

27 Notably, a preservation order (EPrO) does not have a similar review process for issues of conflicting international law.[83] The European Commission has reasoned that a review process is unnecessary because such an order "does not result in data disclosure and therefore does not give rise to similar concerns."[84] EPrOs, however, may be challenged as incomplete, incorrect, or de facto impossible to execute.[85]

c) EU Approach to Conflict of Law Issues Specific to the U.S.

28 To address conflict of law issues specific to the United States, and to complement the e-Evidence proposals, the European Commission is also working to negotiate an international agreement with the United States.

29 On June 6, 2019 the European Council adopted two mandates authorizing the European Commission to negotiate on behalf of EU an agreement with the United States facilitating access to e-evidence for the purpose of judicial cooperation in criminal matters[86] and to participate in the negotiations in the Council of Europe on a second additional protocol to the Cybercrime Convention.[87] Both mandates aim to facilitate the access to e-evidence, such as e-mails or documents located on the cloud, to be used in criminal proceedings. If later concluded, the goals of the mandates will complement the EU framework on access to e-evidence currently being discussed by the EU institutions and on which the European Council has adopted its position in December 2018 and March 2019.[88] As part of the negotiating mandates, the European Council emphasized in its negotiating directives the need for the agreements to be compatible with the EU legislation on access to e-evidence currently being discussed. The European Council also underscored its wish to be closely involved in the preparation and conduct of these negotiations.[89] Considered together with the CLOUD Act, the European Council's initiative thus contemplates several layers of international agreements, including the Draft e-Evidence Direc-

72 *Id.*
73 Regulation Memorandum, *supra* note 57, at 20.
74 *Id.* at 19.
75 Regulation, *supra* note 68, art. 55.
76 Regulation Memorandum, *supra* note 57, at 19.
77 *Id.*
78 *Id.* at 21–22.
79 *Id.* at 22. The Commission emphasizes that the governing court will consider whether conflicting law is intended to protect fundamental rights or interests related to national security or defense, or if it is simply an attempt to "shield illegal activities from law enforcement requests." *Id.*
80 *Id.*
81 *Id.*
82 *Id.*
83 *Id.*
84 *Id.*
85 *Id.* at 20.
86 *See* Council Decision authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 9114/19 available at https://data.consilium.europa.eu/doc/document/ST-9114-2019-INIT/en/pdf (last visited July 23, 2017).
87 *See* Council Decision authorizing the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 9116/19 available at https://data.consilium.europa.eu/doc/document/ST-9116-2019-INIT/en/pdf (last visited July 23, 2017).
88 *See* Press Release, European Council (March 8, 2019), available at https://www.consilium.europa.eu/en/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/(last visited July 23, 2019).
89 *See* Addendum to the Recommendation for a Council Decision authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 9666/19 available at https://data.consilium.europa.eu/doc/document/ST-9666-2019-INIT/en/pdf (last visited July 33, 2019) Addendum to the Recommendation for a Council Decision authorizing the European Commission to participate, on behalf of the European Union, in negotiations on a Second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 9664/19, available at https://data.consilium.europa.eu/doc/document/ST-9664-2019-INIT/en/pdf (last visited July 23, 2019).

tive and Regulation, the Cybercrime Convention, and additional bilateral agreements.

V. Conclusion

30 The CLOUD Act represents an initial effort to address the challenges of cross-border data access by law enforcement. Although aspects of the Act may precipitate conflict-of-law situations for providers-such as the requirement that providers subject to U.S. jurisdiction must disclose data stored outside the United States-other aspects of the law are intended to mitigate such conflicts, including the procedure for bilateral agreements and the opportunity for providers to challenge orders on the basis of international comity.

31 Meanwhile, the EU's initiatives on cross-border data access have involved many of the same elements, such as a procedure for comity-based challenges, even if the jurisdictional reach and other elements of the initiatives differ. Further engagement between the United States and EU, as embodied in the European Council's recent mandates to facilitate cross-border access to e-evidence in criminal matters, will be important to build on the CLOUD Act and e-Evidence initiative, and serve as a link between both.

Alexander A. Berengaut

Partner in Covington & Burling LLP's Washington DC office.

cross-border disputes, with an emphasis on matters involving cybersecurity, data privacy, and electronic surveillance.

He represented Microsoft in the Microsoft Ireland case that led to the enactment of the CLOUD Act.

https://www.cov.com/en/professionals/b/alexander-berengaut

Dr. Lars Lensdorf

Partner in Covington's Frankfurt office.

IT and outsourcing agreements, matters of digitalization and industry 4.0, including online procurement platforms, IT-compliance matters (including cybersecurity) as well as data protection.

https://www.cov.com/en/professionals/l/lars-lensdorf

Case Law

USA: Unconstitutional Discrimination By Trump's use of Twitter's Blocking Function

U.S. Constitution First Amendment

1. The evidence of the official nature of the Account is overwhelming. Therefore, once the President has chosen a platform and opened up the interactive features of his account to the public at large, he is not entitled to censor selected users because they express views with which he disagrees.

2. While the President's tweets can accurately be described as government speech, the retweets, replies, and likes of other users in response to his tweets are not government speech under any formulation. Therefore, extending the government speech doctrine in the way urged by President Trump would result in unconstitutional misuse by silencing the expression of disfavored viewpoints under the guise of the government speech doctrine. ***(all ed.)***

Court of Appeals for the 2nd Circuit, decision of 9 July 2019 by Parker, Hall and Droney, Circuit Judges – Knight First Amendment Institute, et al v. Donald J. Trump, et al. [18-1691-cv]

Facts:

Plaintiffs Buckwalter, Cohen, Figueroa, Gu, Neely, Papp, and Pappas ("Individual Plaintiffs") are social media users who were blocked from accessing and interacting with the Twitter account of President Donald J. Trump because they expressed views he disliked. The Knight First Amendment Institute at Columbia University is an organization alleging a right to hear the speech that the Individual Plaintiffs would have expressed had they not been blocked. The Plaintiffs sued President Trump along with certain White House officials, contending that the blocking violated the First Amendment.

President Donald J. Trump appeals from a judgment of the United States District Court for the Southern District of New York (Buchwald, *J.*) concluding that he engaged in unconstitutional viewpoint discrimination by utilizing Twitter's "blocking" function to limit certain users' access to his social media account, which is otherwise open to the public at large, because he disagrees with their speech. We hold that he engaged in such discrimination and, consequently, affirm the judgment below.

The salient issues in this case arise from the decision of the President to use a relatively new type of social media platform to conduct official business and to interact with the public. We do not consider or decide whether an elected official violates the Constitution by excluding persons from a wholly private social media account. Nor do we consider or decide whether private social media companies are bound by the First Amendment when policing their platforms. We do conclude, however, that the First Amendment does not permit a public official who utilizes a social media account for all manner of official purposes to exclude persons from an otherwise-open online dialogue be-