Storm on the Horizon:

HOW THE U.S. CLOUD ACT MAY INTERACT WITH FOREIGN ACCESS TO EVIDENCE AND DATA LOCALIZATION LAWS

Shelli Gimelstein

DATA Catalyst

TABLE OF CONTENTS

I. INTRODUCTION

Frustrated by the complex and inefficient process of obtaining online data stored by technology companies around the world, the U.S., EU, and numerous other governments have recently enacted legislation making it easier for them to access users' data in connection with criminal investigations. As a result of the U.S. Clarifying Legal Overseas Use of Data Act ("CLOUD Act")[1], the EU's General Data Protection Regulation ("GDPR"), and various countries' data protection and localization laws, technology companies—in particular, online service providers—face rapidly shifting legal landscapes and practical considerations underlying their decisions about where to store user data. U.S.-based providers have particular cause for concern: while the Stored Communications Act (SCA) previously blocked them from disclosing U.S.-held communications content requested by foreign governments, the CLOUD Act amended the SCA to permit foreign governments that have entered into executive agreements with the U.S. to directly serve providers with orders to produce data stored anywhere in the world.

The CLOUD Act emerged in the wake of *Microsoft Ireland*, a 2018 Supreme Court case about U.S. law enforcement's ability to compel U.S. technology companies to provide them with user data stored overseas.[2] Because the case was mooted by the CLOUD Act, the Supreme Court ultimately never addressed the key issue in the case: whether the physical location of data is the appropriate test for determining whether the government should have jurisdiction over it and therefore be able to access it. Through the CLOUD Act, Congress removed jurisdictional barriers to accessing data in an effort to harmonize global law enforcement efforts and facilitate sharing data with qualifying foreign governments (QFGs), particularly in light of the delays and inefficiencies of the existing Mutual Legal Assistance and letters rogatory process. The U.S. and the UK have already begun negotiations leading to an executive agreement, and countries like Australia will likely follow. However, the UK, along with the EU and numerous countries like Australia and India, have passed or are considering passing legislation that could pose a major obstacle toward becoming a QFG, depending on how the U.S. government interprets the certification criteria in Section 2523 of the CLOUD Act.

From the perspective of U.S. providers, a QFG's domestic laws governing data privacy are particularly important because they affect the extent to which companies can legally protect their non-U.S. customers' information. The CLOUD Act permits a provider to file a motion to modify or quash U.S. legal process if it reasonably believes that: 1) the customer or subscriber is not a U.S. person and does not reside in the U.S.; and 2) the required disclosure would create a material risk of violating the laws of a qualifying foreign government.[3] If the QFG has strong procedural safeguards in place—such as requiring probable cause and particularity for search warrants seeking user data—then technology companies will have grounds to challenge requests for non-U.S. users' data that they view to be unjustified or improperly executed. If the country does not have privacy-protective laws, however, the company will have little recourse and cannot shield its customers' information. This can erode customer trust in the company and harm its reputation, as well as open the door to potentially time-consuming, costly, and legally complex requests for data in the future.

---

1 Clarifying Lawful Overseas Use of Data Act, H.R. 1625, 115th Cong. div. V (2018) (enacted) (to be codified in scattered sections of 18 U.S.C.) [hereinafter "CLOUD Act"].

2 The Supreme Court heard oral arguments in the government's appeal of the Second Circuit's 2016 decision in *Microsoft*. The Court held that jurisdiction over data was governed by its physical location, and because the requested data was stored overseas, it was beyond the reach of an SCA warrant. See Microsoft Corp. v. United States (In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 197, 209 (2d Cir. 2016), *certiorari granted*, United States v. Microsoft Corp. (*Microsoft Ireland*), No. 17-2, slip op. at 3 (Apr. 17, 2018) (per curiam) (vacating and remanding judgment).

3 18 U.S.C. § 2713(b)(2).

Much uncertainty remains about how the U.S. will interpret Section 2523 of the CLOUD Act, which sets forth certification criteria for QFGs, as well as how many countries will ultimately enter into executive agreements with the U.S. The process of becoming a QFG may require substantial overhaul of a country's existing legal regime governing law enforcement access to data, and the government may have to address a flawed record on privacy, civil liberties, and free speech in order to gain the approval from the U.S. Attorney General and Congress. However, there are substantial incentives for becoming a QFG. Requiring companies to store data locally may make it easier for the government to access, but providers – many of which are U.S.-based companies – may refuse to comply and simply move their business out of the country. The more feasible alternative for getting access to user data for investigations and other government purposes is to enter into executive agreements with the U.S. in order to directly serve process upon the providers that hold it.

The UK and the EU recently passed legislation similar to the CLOUD Act, authorizing law enforcement officials to issue cross-border data requests to technology companies that operate within their jurisdiction but store data overseas. The UK and Australia have also proposed legislation that may require communications providers, including U.S. companies, to decrypt devices in order to produce data for law enforcement. This paper assesses potential conflicts between these pieces of legislation and U.S. law that may pose obstacles to entering executive agreements in the future. I will also consider how strictly the U.S. will enforce the CLOUD Act's requirements for QFG status, including commitment to free speech and an open internet.

Ultimately, strict enforcement of the CLOUD Act requirements will leave few, if any, countries qualified to enter into executive agreements. Therefore, it will not be expedient for the U.S. to strictly enforce these requirements, though this may create privacy concerns for U.S. companies and citizens. The UK will likely be approved for an executive agreement, setting the stage for an executive agreement with the EU once lawmakers determine whether the U.S. can and should enter into individual agreements with EU countries or whether one agreement with the EU as a whole will be legally sufficient for both authorities to be able to access the data they need. Australia has also expressed interest in striking an executive agreement with the U.S. as soon as possible.[4] The terms of future agreements will likely be affected by how U.S. courts interpret foreign laws and apply the comity analysis in the first sets of challenges to CLOUD Act orders in the months to come.

4 David Wroe, *Police could access US cloud data under planned crime-fighting deal*, The Sydney Morning Herald (Apr. 8, 2018), https://www.smh.com.au/politics/federal/police-could-access-us-cloud-data-under-planned-crime-fighting-deal-20180407-p4z8c0.html.

II. THE CLOUD ACT

A. Certification Requirements

In order for a QFG to enter into an executive agreement with the U.S., the Attorney General must certify that the foreign nation's domestic law "affords robust substantive and procedural protections for privacy and civil liberties" in its data-collection activities, and includes "appropriate" procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons." The executive agreement does not require providers to be capable of decrypting data, but it does not prevent providers from voluntarily building decryption capabilities into their devices or networks.

Within seven days of certifying an executive agreement with a government that meets CLOUD Act standards, the Department of Justice ("DOJ") must provide Congress with the text of bilateral agreement, along with an explanation as to why that country and the orders authorized under the agreement meet CLOUD Act requirements. The DOJ must also print "any determination or certification" regarding CLOUD Act agreements in the federal register. After that, Congress has 180 days to decide whether to pass a law nullifying the agreement.[5] The CLOUD Act does not give Congress the ability to modify or make recommendations for the terms of the agreement.

B. Limitations on Orders

1. QFG Requests

Once a QFG has entered into an executive agreement with the U.S., under Section 2523(b)(3)(D), it may issue orders directly to U.S. providers, as long as these orders:

- are for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism
- identify a specific person, account, or other identifier that is the object of the order
- are premised on a "reasonable justification based on articulable and credible facts, particularity, and severity regarding the conduct under investigation"
- do not intentionally target a U.S. person (or person located in the U.S.) or target a non-U.S. person with the intention of obtaining information about a U.S. person
- are issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution or a "serious "crime" (including terrorism)
- comply with the domestic law of the issuing country
- are not used to infringe freedom of speech; and
- satisfy additional requirements for real-time communications captured by wiretap.

5 18 U.S.C. § 2523(d)(2).

Additionally, under Section 2523(b)(3)(D)(v), foreign governments' orders "shall be subject to review or oversight by a court, judge, magistrate, or other independent authority." However, the CLOUD Act does not compel U.S. providers to comply with any foreign order. Any obligations for providers to comply must arise under foreign law.[6]

As a preliminary matter, there are several areas of ambiguity in these criteria. First, it is unclear whether the CLOUD Act requires that foreign governments receive judicial authorization from their own courts for data requests before they can be served on U.S. providers. Section 2523(b)(3)(D)(v) could be interpreted as requiring only *ex post* oversight through, for example, allowing the subject of an order to challenge it in court after disclosure has already occurred.[7] If this is the case, then the providers served with the order would be the only entities responsible for ensuring that orders are sufficiently specific, are issued for a legitimate purpose, do not target U.S. persons, and otherwise meet 2523(b)(3)(D) requirements. From a procedural and practical standpoint, this situation is problematic for two reasons. First, providers—particularly smaller companies without a large legal department—may not have adequate personnel or expertise to make these legal determinations, which involve complex questions of criminal procedure and foreign law, as well as questions of fact that would require substantial information about the circumstances of the investigation for which the request has been issued. Second, providers would have to interpret Section 2523(b)(3)(D) requirements for each order on a case-by-case basis without guidance from courts, producing inconsistent results that, depending on that provider's policies, affected users may not have a means of challenging. Absent explicit provisions in an executive agreement requiring judicial review of all orders before serving them upon a provider, the CLOUD Act potentially exposes U.S. providers and their customers to a large volume of orders that may not meet basic requirements of due process.

The CLOUD Act also provides that orders must not be "used to infringe on the freedom of speech," but does not specify whether this refers to U.S. principles of free speech, which are considerably broader than those of many countries with which the U.S. will likely enter into executive agreements. For example, the UK forbids a number of forms of speech that enjoy protection under the First Amendment in the U.S., including sending messages over a public communications network that are "grossly offensive or of an indecent, obscene or menacing character," or intended to cause "annoyance, inconvenience or needless anxiety to another."[8] A UK law enforcement request for a UK citizen's "grossly offensive" messages, even if sought in connection with a serious crime, may have the effect of deterring or infringing on free speech as it is understood in the U.S. An additional factor that may complicate the analysis of which country's free speech laws apply is where the targeted individual was located at the time when they sent the messages. Given the varying circumstances that will accompany each individual request, U.S. providers will effectively be forced to have different standards for when to protect and when to disclose different users' communications information. This may prevent them from developing consistent principles and policies through which they can build trust with their users.

2. Challenging Orders in Court

If a provider has determined that a CLOUD Act request from a U.S. law enforcement agency does not meet Section 2523(b)(3)(D) requirements, the provider may challenge such a notice in a court of law, as long as:

6 Jim Garland, Alexander Berengaut and Katharine Goodloe, *CLOUD Act Creates New Framework for Cross-Border Data Access*, Covington & Burling: Inside Privacy (Mar. 26, 2018), https://www.insideprivacy.com/cloud-computing/cloud-act-creates-new-framework-for-cross-border-data-access/.

7 Greg Nojeim, *Cloud Act Implementation Issues*, Lawfare (Jul. 10, 2018), https://www.lawfareblog.com/cloud-act-implementation-issues.

8 Peter Swire and Justin Hemmings, *Recommendations for the Potential U.S.-UK Executive Agreement Under the Cloud Act*, Lawfare (Sept. 13, 2018), https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act; see Section Communications Act 2003 § 127(1).

1. the person who is the subject of the request is not a United States citizen; and
2. such disclosure would cause a material risk of the service provider violating the laws of the foreign government.

The court may modify or quash the legal process, as appropriate, if:

1. the required disclosure would cause the provider to violate the laws of a qualifying foreign government;
2. based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and
3. the customer or subscriber is not a United States person and does not reside in the United States. In evaluating the motion to quash, the court will consider the interests of both governments, whether other means of obtaining the data exist, and the likely penalties the provider and its employees may suffer "as a result of inconsistent legal requirements imposed on the provider."[9]

In order to prevent courts from striking down CLOUD Act requests due to conflicts with foreign law, the DOJ will likely determine the citizenship of the target of a request before deciding on the appropriate legal process for obtaining their data.[10]

In contrast, the CLOUD Act does not provide a way for providers to challenge QFGs' requests for non-U.S. customer data in court, and foreign governments may not be scrupulous in determining the citizenship of their targets. In determining whether a QFG's request meets Section 2523(b)(3)(D) requirements, a provider is effectively forced to apply that country's laws on issues such as evidence, criminal procedure, and freedom of speech. Providers may seek to challenge such requests in foreign courts, which would then be forced to interpret the CLOUD Act with little guidance. In this situation, courts would likely have three options. The most straightforward and privacy-protective approach would be to impose the U.S. standards set forth in Section 2703 on the request. Second, applying similar factors to those in U.S. common law, courts could create a comity exception that permits the government to access the data, perhaps in the event that the data belongs to a citizen of that nation and there are minimal U.S. ties to the data or person in question. Finally, courts could delay approval until U.S. and foreign governments provide further clarity about the standards that should apply to such a request.

Regardless of the approach courts take to evaluating motions to quash CLOUD Act requests, there may be negative consequences for customers' data privacy. While the specificity, particularity, and proportionality requirements for orders under Section 2523(b)(3)(D) provide some protection for non-U.S. targets of an order, the QFG's laws may not provide for due process for targets of investigations, including judicial oversight and authorization for orders, probable cause requirements, and other procedural protections guaranteed under the U.S. Constitution. This is true of both the UK and Australia—the governments most likely to enter executive agreements with the U.S. in the near future—even though they may have substantially more legal protections for targets of orders than non-democratic, non-Western governments. This means providers may be forced to apply a double standard in how they store and safeguard U.S. and non-U.S. customers' data. Section III will discuss the major flaws in these governments' domestic laws that should be addressed in negotiations leading to an executive agreement, so as to minimize the ethical, legal and technical concerns that may rise when U.S. courts and technology companies are required to apply and adhere to foreign laws.

9 *Id.*

10 Nojeim, *supra* note 7.

3. U.S. Requests for Data Located in a Non-QFG

While Section 2703(h) sets forth specific standards for evaluating requests for non-U.S. persons' data when these conflict with the laws of a QFG, the CLOUD Act calls for courts to apply common law comity standards when providers seek to quash U.S. requests for data stored in countries with which the U.S. does not have an executive agreement.[11] These would likely be the same common law comity standards that currently apply to SCA warrants that involve U.S. persons or any person inside the U.S., which means that a provider could challenge such a request even if the data belongs to a customer or subscriber who is a U.S. citizen or resides in the U.S.

Courts may look to cases involving foreign enforcement of domestic subpoenas when conducting a conflict of laws analysis for challenges to CLOUD Act orders. Subpoenas provide a useful analogue since they apply to all data, regardless of location, over which the entity subject to the order has custody or control. A court would likely evaluate a request using the comity factors set forth in *Société Nationale Industrielle Aérospatiale*, where the Supreme Court evaluated whether a foreign company could be compelled to produce documents in the U.S. litigation based on: 1) the importance of the documents or other information requested; 2) the degree of specificity of the request; 3) whether the information originated in the U.S.; 4) whether there were alternative means of obtaining the information; and 5) whether noncompliance with the request would undermine U.S. or foreign interests.[12] In weighing U.S. and foreign interests in data, courts may also rely on cases like *Bank of Nova Scotia*, where the Eleventh Circuit upheld a subpoena compelling a Canadian bank's Miami branch to produce data stored in the Bahamas, in violation of Bahamian law.[13]

The fifth comity factor will likely be the greatest source of controversy throughout the ongoing implementation of the CLOUD Act and the GDPR—at least before the U.S. and EU enter into an executive agreement. Courts will be forced to weigh U.S. interests in obtaining the data with the EU's interests in protecting data subjects' rights. As discussed in greater detail below, whether courts ultimately order U.S. providers to abide by the GDPR may shape the final terms of any executive agreement that may be entered in the future.

11 18 U.S.C. § 2703(h).

12 Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

13 See In re Grand Jury Proceedings the Bank of Nova Scotia, 740 F.2d 819, 820 (11th Cir. 1984) (finding that the Canadian bank, which was subpoenaed at its Miami office, could be compelled to produce documents held in a Bahamian branch, even though this would violate Bahamian bank secrecy laws, "contrary to the interests of our nation and outweigh the interests of the Bahamas.")

III. POTENTIAL CONFLICTS OF LAW

A. Forced Decryption and the UK Investigatory Powers Act

Under Section 2523(b)(3) of the CLOUD Act, executive agreements "shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data." Congress must review and approve all executive agreements, creating some oversight to ensure this provision is met.[14] However, the CLOUD Act does not explicitly state that beyond the executive agreement, a QFG cannot have any domestic laws that enable it to force providers to decrypt data. It is unclear whether Congress or U.S. courts would treat such a law as a violation of the certification requirements to enter into an executive agreement.

The issue will likely arise in executive agreement negotiations with the UK and Australia, whose legislatures are both expected to pass legislation that could require companies to build mandatory encryption backdoors in their products. For example, the 2016 Investigative Powers Act ("IPA") establishes the conditions for the UK government to compel a company to produce user data, and gives it wide surveillance capabilities, including equipment interference (government hacking) and communications and metadata interception.[15] The IPA also authorizes the government to issue "technical capability notices" that "create obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data." This suggests that internet service providers (ISPs) served with a technical capability notice would have to decrypt user data or create a backdoor through which the government can bypass encryption and access it. Technical capability notices appear to be enforceable against U.S. companies, which may create a conflict with the provision against mandatory decryption in Section 2523(b)(3) of the CLOUD Act. This issue, along with the lack of transparency requirements and judicial oversight for all of the surveillance measures in the IPA, should be a red flag for the U.S. Attorney General in assessing whether the UK has adequate privacy protections to meet the CLOUD Act certification criteria.

For the sake of consistency, future executive agreements should explicitly render these laws inapplicable to requests served upon U.S. providers. However, the U.S. may be unwilling to do so because the DOJ is currently embroiled in a domestic legal dispute over whether it can compel U.S. companies to decrypt certain stored data. In August 2018, the government sought to force Facebook to produce end-to-end encrypted voice conversations sent through Facebook Messenger.[16] According to Facebook, the company can only fulfill the government's request by rewriting the code that currently protects all users' data in order to remove encryption, or by hacking the target's account.[17] While court documents are presently sealed, the DOJ's case likely rests on the argument that encrypted Facebook Messenger content is an electronic

14 Peter Swire and Jennifer Daskal, *What the CLOUD Act means for privacy pros*, International Association of Privacy Professionals (Mar. 26, 2018), https://iapp.org/news/a/what-the-cloud-act-means-for-privacy-pros/.

15 Greg Nojeim and Christine Galvagna, *UK Investigatory Powers Bill Imperils Public Safety by Undermining Data Sharing with the US*, Ctr. Democracy & Tech. (Sept. 6, 2016), https://cdt.org/blog/ukinvestigatory-powers-bill-imperils-public-safety-by-undermining-data-sharing-with-the-us/.

16 John Villasenor, *Decrypting The Compelled Decryption Fight Over Facebook Messenger*, Forbes (Aug. 22, 2018), https://www.forbes.com/sites/johnvillasenor/2018/08/22/decrypting-the-compelled-decryption-fight-over-facebook-messenger/#7cb62c1958ea.

17 Dan Levine and Joseph Menn, *Exclusive: U.S. government seeks Facebook help to wiretap Messenger – sources*, Reuters (Aug. 17, 2018), https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D.

communication subject to disclosure under the Electronic Communications Privacy Act pursuant to a valid Stored Communications Act warrant.[18] If the DOJ succeeds in persuading the court to require Facebook to decrypt the target's voice messages, it could give momentum to legislative proposals like Compliance with Court Orders Act of 2016, which was proposed by Senators Dianne Feinstein (D-CA) and Richard Burr (R-NC) shortly after Apple refused to comply with a court order to decrypt the iPhone of the suspects in the San Bernardino mass shooting. While that bill ultimately failed to pass, the issue remains of great interest to lawmakers frustrated with technology companies' lukewarm attitudes towards assisting with law enforcement investigations. As a result, the U.S. government may not consider it a priority to address other governments' domestic mandatory decryption laws, even if the CLOUD Act prohibits such provisions from being included in executive agreements.

B. UK Overseas Production Orders Bill

The UK Parliament is currently considering enacting the Crime (Overseas Production Orders) Bill, which was passed by the House of Lords on November 20, 2018 and is currently due for a third reading before the House of Commons.[19] The Bill enables British law enforcement officers to issue "overseas production orders" demanding access to evidence held outside the UK.[20] Judges may approve such orders if they believe "there are reasonable grounds for believing that an indictable offence has been committed and proceedings in respect of the offence have been instituted or the offence is being investigated" or "the order is sought for the purposes of a terrorist investigation."[21] Mirroring the extraterritorial reach of the CLOUD Act, Section 6(4) of the Bill requires providers to comply with an overseas production order regardless of where it stores the requested electronic data, and "has effect in spite of any restriction on the disclosure of information."

Negotiations between the U.S. and UK leading up to an executive agreement will likely focus on whether this bill is compliant with the CLOUD Act's Section 2523 requirements. First, several provisions of the UK Bill prevent the U.S. from reviewing orders issued by British law enforcement. Section 8 permits a judge to include a non-disclosure requirement in an overseas production order, which requires the person against whom the order is made to not disclose the order or its contents—including, potentially, outside counsel or the U.S. DOJ. This may run afoul of the provision in the CLOUD Act requiring that QFGs have "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government," as well as Section 2523(4)(K), in which the U.S. "reserve[s] the right to render the agreement inapplicable as to any order for which the United States Government concludes the agreement may not properly be invoked." Additionally, non-disclosure requirements may prevent the target from being notified about the order and thus being able to challenge it, even though Section 7 of the Bill allows "any person affected by the order" to apply to modify or revoke it.[22] Finally, the lack of transparency for orders subject to non-disclosure violates the judicial review requirements for foreign governments' orders in Section 2523(b)(3)(D)(v).

18 Villasenor, *supra* note 16.

19 *See* Crime (Overseas Production Orders) Bill 2017-19, HL Bill [307].

20 Swire and Hemmings, *supra* note 8.

21 Crime (Overseas Production Orders) Bill, *supra* note 19.

22 Swire and Hemmings, *supra* note 8.

C. EU Legislation

1. General Data Protection Regulation

The GDPR, which went into effect May 25, 2018, enacted a number of sweeping changes to how providers must legally store and process individuals' personal data inside the EU.[23] Besides mandating privacy safeguards and technical measures for personal data, such as de-identification and erasure upon request, the GDPR places conditions on providers' ability to transfer personal data to third countries.[24] The GDPR applies to data belonging to all EU persons, including citizens of other countries, which means that CLOUD Act requests by the U.S. government for the data of U.S. citizens that reside in the EU will have to comply with GDPR data transfer rules. Currently, there are several areas of conflict between the GDPR and the CLOUD Act that will make compliance difficult, at least unless the two governments enter an executive agreement clarifying how these conflicts of law are to be resolved.

First, as a foreign law, the CLOUD Act may not provide a sufficient legal basis for the lawful transfer of data outside the EU. Under GDPR Art. 48, court-ordered international data transfers must be "based on an international agreement such as a Mutual Legal Assistance Treaty (MLAT), in force between the requesting third country and the Union or a Member State."[25] The CLOUD Act is not an international agreement. Nor does it qualify as a "legal basis" within the meaning of GDPR Art. 6, which refers specifically to EU or member state law as the two sources of a legal basis for data processing.[26] Moreover, Recital 115 of the GDPR states that the extraterritorial application of "judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State," is contrary to both the GDPR and international law.[27]

GDPR Art. 49 permits exceptions to this rule in two situations: 1) "where disclosure is necessary for an important ground of public interest recognised in Union or Member State law to which the controller is subject," and 2) if disclosure is necessary for "compelling legitimate interests pursued by the controller which are not overridden by the interests of the data subject."[28] While the need to obtain data in connection with serious criminal investigations could arguably meet at least one of these standards,[29] Art. 49 is likely to be strictly interpreted, and they are unlikely to find that providers' interests in avoiding sanctions for noncompliance with U.S. court orders outweigh the privacy interests of data subjects. In the absence of an EU-US executive agreement or a wholesale exception to GDPR Art. 48 for CLOUD Act requests, providers subject to the GDPR will be forced to violate either U.S. or EU law each time they are compelled to produce U.S. citizens' data.

23 *See* Council Regulation 2016/679, 2016 O.J. (L 119) [hereinafter "GDPR"].

24 *Id.* art. 46.

25 *Id.* art. 48.

26 *Id.* art. 6.

27 *Id.* recital 115.

28 *Id.* art. 49.

29 Jennifer Daskal, *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, Stanford Law Review Online (May 2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.

Although this topic is outside the scope of this paper, it is worth noting that potential conflicts between the CLOUD Act and the GDPR could be further complicated by whether the U.S. decides to sign separate agreements with different EU countries. It is unclear what the parameters of those agreements would be in light of a concurrent U.S.-EU agreement.

2. E-Evidence Directive

The EU E-Evidence Directive, which was promulgated on April 17, 2018,[30] mirrors the CLOUD Act in that it allows EU authorities to serve transnational European production orders ("EPO") upon online service providers in order to gather evidence for criminal proceedings. However, only providers with a "substantial connection to the Union" based on "the existence of a significant number of users in one or more Member States, or the targeting of activities towards one or more Member States" are required to comply with the Directive.[31] The Directive applies broadly to providers of "variety of computing resources such as networks, servers or other infrastructure, storage, apps and services that make it possible to store data for different purposes," as well as "digital marketplaces that allow consumers and/or traders to conclude transactions via online sales or service contracts with traders."[32] Under the Directive, a prosecutor or judge in any EU state may directly serve an EPO upon any service provider, bypassing the authorities of the member state that hosts the provider. The service provider must produce the requested data within 10 days of receiving the warrant, or within six hours of the request in urgent cases. Since the Directive only applies to stored data, member states cannot serve prospective EPOs concerning future data flows. This means real-time communications are excluded from the scope of the Directive and remain subject to the various national legal frameworks of EU member states.

To facilitate compliance with EPOs, the Directive requires all providers operating in the EU to designate a legal representative responsible for receiving, complying with and enforcing EPOs on behalf of the service provider—a potentially onerous cost for providers that may have EU customers but do not have a physical presence there.[33] Mirroring the extraterritorial reach of the CLOUD Act, the Directive also applies to providers that store data outside the EU but offer services and are established or represented within the EU.[34] This means that until the U.S. and EU negotiate and enter into an executive agreement, non-EU providers served with an EPO may be forced to choose between violating their own country's laws in order to comply or facing penalties for non-compliance.

The Directive lacks a number of procedural safeguards required for the EU to be certified by the Attorney General as a QFG. First, it provides no process by which individuals whose data is being requested can challenge an EPO, and it does not provide legal remedies for individuals whose data was improperly requested or mishandled. Second, it does not

30 *See* 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 (April 17, 2018).

31 *See id.*

32 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 (April 17, 2018).

33 *See* 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, *supra* note 30 (noting that Germany has already adopted its own version of this law through the "Network Enforcement Act," which requires social network providers to designate a person in Germany to receive law enforcement requests and imposes sanctions of up to 500,000 euros for failure to name a representative or respond to law enforcement requests. In contrast, Belgium does not require providers to have a local representative but directly brings foreign providers into domestic legal proceedings for noncompliance with law enforcement requests.)

34 Alexandra Brzozowski, *E-Evidence: A threat to people's fundamental rights?*, Euractiv (Dec. 5, 2018), https://www.euractiv.com/section/data-protection/news/e-evidence-a-threat-to-peoples-fundamental-rights/1296698/.

establish consequences for noncompliance with EPOs or violations of the procedural rules governing EPOs, leaving it up to member states to determine what sanctions to impose and whether to allow improperly obtained e-evidence to be admitted in court.[35] However, the Directive does allow providers to challenge abusive orders by member states or orders that violate the EU Charter, although this burdens providers, particularly smaller smart-ups, by forcing them to conduct a private legal analysis to assess whether the order complies with the Charter.[36] Absent amendments or guidance on how member states should implement the Directive, this will likely run afoul of the CLOUD Act's requirement that a QFG's domestic laws must afford robust substantive and procedural protections for privacy and civil liberties.

D. Australia's Assistance and Access Act

In an effort to expand law enforcement access to data without resorting to data localization measures, Australia recently passed legislation that may force technology companies to decrypt devices on demand in order to produce evidence for criminal investigations. On December 6, 2018, the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 received Royal Assent and passed through both houses of Parliament.[37] Under the Act, communications providers and device manufacturers, including both domestic and foreign companies, may either voluntarily provide assistance to Australian intelligence and law enforcement agencies under a "technical assistance request," or they may be compelled to provide assistance under a "technical assistance notice." Law enforcement and intelligence agencies may also issue "technical capability notices" to require these companies to "do acts or things to ensure the provider is capable of giving help to ASIO and interception agencies where the Attorney-General is satisfied that it is reasonable, proportionate, practicable and technically feasible."

There are three elements of the Act that may create a problem if and when Australia seeks to enter into an executive agreement with the U.S. First, while the Act does not go as far as the CLOUD Act in explicitly stating that law enforcement can request data irrespective of the location in which it is stored, several provisions in the Act suggest that it has a similar effect. The Act is "assumed to apply extra-territorially" and "the need for a warrant or authorisation applies equally to onshore and offshore providers."[38] The Act does not provide any grounds for jurisdiction over these foreign companies. The Act also lacks built-in procedures and safeguards to ensure due process with respect to issuing and challenging requests; there is no process of judicial authorization, nor is there a mechanism for challenging erroneously issued orders or execution that exceeds the scope of the order. All of this may prevent Australia, at least initially, from meeting the CLOUD Act certification criteria.

Second, the Act's emphasis on the use of encryption by criminals and terrorists and its deleterious effect on law enforcements' intelligence-collecting capabilities suggests that technical capability notices will be used to circumvent encryption measures. Although the Act states that a provider cannot be required to "implement or build a systemic

35 Vanessa Franssen, *The European Commission's E-Evidence Proposal: Toward an EU-Wide Obligation for Service Providers to Cooperate with Law Enforcement?*, European Law Blog (Oct. 12, 2018), http://europeanlawblog.eu/2018/10/12/the-european-commissions-e-evidence-proposal-toward-an-eu-wide-obligation-for-service-providers-to-cooperate-with-law-enforcement/.

36 *Id.*

37 Tom Westbrook and Karishma Luthria, *Australia passes bill to force tech firms to hand over encrypted data*, Reuters (Dec. 5, 2018), https://www.reuters.com/article/us-australia-security-data/australia-passes-bill-to-force-tech-firms-to-hand-over-encrypted-data-idUSKBN1O42SR.

38 Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, sch. 1-13.

weakness or vulnerability into a form of electronic protection," this is precisely what circumventing encryption would entail. When a provider or device manufacturer weakens or disables encryption on one device in order to produce stored information, they may not be able to test and control the scope of the new vulnerability while responding to a time-sensitive notice. Moreover, any new vulnerability built into a device in order to provide effective assistance to law enforcement can be discovered and replicated system-wide on other devices, affecting users and systems not targeted by the notice. Ultimately, in order to comply with the Act, providers and manufacturers will be forced to create less secure devices, weakening the strong encryption that protects both individual customers and national infrastructure from hackers and other bad actors seeking to improperly access and/or access sensitive data. Similarly to the decryption provision in the UK's IPA, this appears to contravene the CLOUD Act certification criteria, which prohibit executive agreements from imposing decryption obligations on providers and require them to have adequate legal protections for privacy and civil liberties.

Third, the Act enables the Australian government to demand assistance from foreign communications providers not only for its own domestic purposes, but also for "assisting enforcement of the criminal laws in force in a foreign country." For example, China could request Australia's assistance with a criminal investigation of a Chinese citizen who used Facebook Messenger while in Australia. The Facebook data could be stored in the U.S., putting it outside China's reach absent an executive agreement or a Mutual Legal Assistance treaty with the U.S. An executive agreement under the CLOUD Act would enable Australia to serve an order directly upon Facebook, which would have few, if any, options for challenging the order. In the abstract, this would conflict with Section 2523(b)(3)(C), which prohibits a foreign government from issuing "an order at the request of or to obtain information to provide to the United States Government or a third-party government." However, in practice, this provision will be difficult to enforce in light of the limited grounds for providers to move to quash an order, particularly when multiple countries are involved in or have jurisdiction over elements of a criminal investigation.

The possibility of non-QFGs accessing providers' data indirectly via Australian intelligence agencies will likely be a significant issue in future negotiations between the U.S. and Australia concerning an executive agreement. The Act remains subject to further amendment and review until April 2019.[39] It remains to be seen whether lawmakers clarify the language around systemic weaknesses or otherwise modify the Act to enable Australia to meet the certification criteria for entering into an executive agreement with the U.S.

E. Data Localization Laws

The CLOUD Act sets forth a number of requirements in order for a foreign government to qualify to enter into an executive agreement. The requirement of a "commitment to an open internet," defined as a "demonstrated commitment to promote and protect the free flow of information across borders and open Internet," poses a particular obstacle to certification for countries with data localization requirements. Setting aside the troubling ambiguities and procedural deficits of the CLOUD Act discussed above, the successful implementation of executive agreements could provide a substantial incentive for countries to avoid adopting some of the most dangerous policies for privacy, freedom of speech and technological growth: data localization requirements.

39 Julian Lincoln, Anna Jaffe and Lara Howden, *The Assistance and Access Act 2018: The Crypto Wars' Final Act for 2018*, Herbert Smith Freehills (Dec. 11, 2018), https://www.herbertsmithfreehills.com/latest-thinking/the-assistance-and-access-act-2018-the-crypto-wars-final-act-for-2018.

Countries adopt data localization laws to restrict the flow of data, either by prohibiting its transfer outside of the country or requiring that providers who process their citizens' data store it exclusively in data centers located on their soil. This makes it easier for domestic intelligence agencies to demand access to that data, whether for the purposes of a criminal investigation or, in the case of countries like China and Russia, in order to spy on their citizens' communications. The privacy implications of data localization laws reach beyond foreign citizens. For example, communications or transactions between U.S. and non-U.S. citizens would have to be stored on these foreign servers as well, exposing U.S. citizens' data to largely unfettered access by foreign governments that do not afford the same level of protection for civil liberties and privacy guaranteed under U.S. law.

Data localization policies also carry substantial legal uncertainty and financial costs for providers, particularly smaller local companies that, unlike Google and Amazon, cannot afford to build data centers around the world. Some countries have adopted data localization in an effort to spur homegrown economic activity and innovation, or to give local companies a competitive advantage.[40] However, studies show that these policies have the opposite economic effect. According to Leviathan Security Group, providers based in countries that require them to store data within their borders pay 30-60% more for their computing needs than if they were free to store data where it would be more cost-effective to do so.[41] The European Centre for International Political Economy (ECIPE) conducted a study of seven cloud providers with datacenters in twelve countries and found that within the EU, businesses that move their servers outside the region could save more than 36% in server costs.[42] Local businesses in countries without publicly available cloud computing providers face even greater costs; they must either resort to using non-public cloud computing resources or must purchase and maintain their own data storage infrastructure.[43] As a result, some providers may avoid offering their products in countries with data localization laws, particularly if there is reason to believe that storing data abroad may compromise its security and subject customers to surveillance by foreign governments. Forced data localization also has harmful effects at a macroeconomic level. According to ECIPE, economy-wide data localization laws drain between 0.7% and 1.1% of GDP from the economy, causing a loss of output in the general economy that outweighs any benefits derived from forcing businesses to keep their storage operations local.[44]

Finally, data localization deters the development of innovative technologies by limiting providers' ability to optimize and scale their services. One of the benefits behind cloud storage technology—and the reason for its low costs to providers—is that it enables companies to operate globally without establishing a global physical presence.[45] Compliance with data localization forces companies to operate less efficiently, driving up costs for consumers. Additionally, restrictions on data processing prevent companies from analyzing vast swaths of data to develop better products and services: for example,

40 China, in 2016 Top Markets Cloud Computing Country Case Study, Int'l Trade Admin, U.S. Dep't of Commerce, http://trade.gov/topmarkets/pdf/Cloud_Computing_China.pdf.

41 *Quantifying the Cost of Forced Localization*, Leviathan Security Group at 3 (June 24, 2015), https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.

42 Erik van der Marel, Hosuk Lee-Makiyama, and Matthias Bauer, *The Costs of Data Localisation: A Friendly Fire on Economic Recovery*, European Centre for International Political Economy (May 2014), http://ecipe.org/publications/dataloc/.

43 Leviathan Security Group, *supra* note 41.

44 See van der Marel, Lee-Makiyama and Bauer, *supra* note 42.

45 Alexander Savelyev, *Russia's new personal data localization regulations: A step forward or a self-imposed sanction?*, 32 Computer Law & Security Review 128, 139 (2016).

using big data analytics to optimize healthcare delivery, or creating and improving Internet-of-Things (IoT) devices using data collected by sensors on internet-connected, "smart" devices.[46]

A number of countries like Russia and China have adopted strict data localization requirements as part of a broader policy of monitoring, censoring and controlling internet activities and technology companies' operations within their borders, although these countries have outwardly claimed the purpose of their data localization laws is to shield their citizens' data from foreign surveillance.[47] China's 2017 Cybersecurity Law requires all personal information and "important data" concerning "critical information infrastructure"—including public communication and information services, energy, transportation, water resources, finance, public services, [and] e-governance—to be stored locally in mainland China. The data localization law is vague regarding its scope and the entities to which it applies, and has drawn concern from industry groups regarding both compliance costs and potential surveillance by the Chinese government.[48] Meanwhile, Russia has already enforced its localization laws[49] against LinkedIn, which was blocked in 2016 for noncompliance, and sanctioned the German company Telegram for not providing it with decryption keys, as required by Article 10.1 (4.1) of the Russian Data Protection Act.[50] Building the infrastructure and writing the code to transfer personal data from global to local databases can cost companies millions of dollars, but the Roskomnadzor, or the Russian Ministry of Communications, appears to be unconcerned with the resulting economic losses, viewing this as a reasonable "cost of doing business" in Russia.[51] Since it is already highly unlikely that the U.S. would ever enter into an executive agreement with the Russian Federation given the tense relations between the two countries as well as its abysmal record on human rights, it is unlikely that Russia will have an incentive—at least from an external source—to change its data localization policies in the future.

However, other countries have adopted data localization policies recently out of frustration with the inefficiency of obtaining data for investigations from U.S. providers through the Mutual Legal Assistance process, and may be willing to curb these policies, at least for U.S. providers. India is a prime example of a country that is likely eager to enter into an executive agreement with the U.S. but currently falls short of the QFG certification requirements because of its data localization policies for certain industries. Currently, all telecommunications service providers are required to store customer data within India under the Unified License,[52] while financial institutions must do the same for all payment data under the rules of the Reserve Bank of India.[53] The Parliament of India is also considering passing a Data Protection

46 *Id.* at 143.

47 *Id.* at 139.

48 Yuxi Wei, *Chinese Data Localization Law: Comprehensive but Ambiguous*, University of Washington Jackson School of International Studies (Feb. 7, 2018), https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/.

49 *See* Federal Law of the Russian Federation on Information, Information Technologies and Protection of Information 2006, No. 149-FZ.

50 *See* Federal Law of the Russian Federation Amending Certain Legislative Acts of the Russian Federation as to the Clarification of the Processing of Personal Data in Information and Telecommunications Networks 2015, No. 242-FZ; *see also* Sergey Medvedev, *Data Protection & Privacy Laws 2018 / Russian Federation*, Financier Worldwide (Dec. 2018), http://www.gorodissky.com/upload/articles/files/FinancierWorldWide_Data_Protection_2018_Russia.pdf.

51 Savelyev, *supra* note 45 at 142.

52 License Agreement for Unified License, Government of India, Ministry of Communications & IT, Dep't of Telecommunications (2013), http://dot.gov.in/sites/default/files/Unified%20Licence_0.pdf

53 Storage of Payment System Data, RBI/2017-18/153, Reserve Bank of India (Apr. 6, 2018), https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0.

Bill that requires copies of all personal data, as well as all "sensitive personal data," to be stored in India.[54] Before it is willing to consider entering into an executive agreement, the U.S. may require India to make substantial changes to its data localization policies, along with changes to other substantive and procedural laws, such providing for judicial rather than executive authorization for data interception requests.[55]

54 Elonnai Hickock and Vipul Kharbanda, "An Analysis of the CLOUD Act and Implications for India," The Centre for Internet and Society - India (Aug. 22, 2018), https://cis-india.org/internet-governance/files/analysis-of-cloud-act-and-implications-for-india.

55 *Id*. (noting that "[b]ecause the CLOUD Act will allow for local law to be applied if an Executive Agreement is entered into, India's regime of allowing executive authorization for interception requests technically falls within the framework defined by the Act, but it is not clear that this framework will meet the requirement of the domestic law provides robust substantive and procedural protections for privacy and civil liberties. This is particularly true as it has been noted by experts that the shift to a framework of judicial authorization by the U.K in 2016 was motivated by the need to meet the conditions necessary for an executive agreement.").

IV. IMPACT ON PROVIDERS & CONCLUSIONS

The potential conflicts between the CLOUD Act and foreign legislation may delay the finalization of executive agreements that will bring major changes to how providers must handle government requests for data. As discussed above, some foreign governments may be motivated to change their domestic laws—such as adding judicial authorization requirements for court orders—in order to qualify for an executive agreement. However, the most likely outcome is that in light of the many ambiguities in the CLOUD Act as it currently stands, the DOJ will have to provide further guidance on how the law is be implemented and interpreted, both for the sake of potential QFGs and for the providers whose operations will be significantly affected by the new legal regime.

The many dramatic changes in U.S. and foreign data protection, storage, and production laws have already imposed financial and technical burdens on all providers. In particular, smaller companies are hardest hit by the rising costs of compliance, as well as the uncertainty around how these laws will be enforced. As a result of the CLOUD Act and related legislation around the world, many providers will be forced to change how they operate and store data in an inefficient, costly manner because of various legal regimes' requirements for data storage, and because of strategic choices about where to locate the company for the purposes of being served with legal process.

In large part, how providers modify their operations in response to the CLOUD Act will stem from the scope of the definition of "control." Under the CLOUD Act, all email and cloud storage providers with U.S.-based operations now must disclose emails and other stored data within their "possession, custody, or control," regardless of whether the data is stored in the U.S. or abroad. Courts apply the "possession, custody, or control" test by looking at "the degree of ownership and control a corporation exercises over a related entity, whether the two companies operate as one, whether they have common policies, whether one company has access to documents from the other in the ordinary course of business, whether there is an agency relationship, and any overlap in the executives of the two companies."[56] Rather than developing in-house cloud storage infrastructure, most companies—with the exception of tech giants like Amazon and Google that also offer cloud services—use third-party cloud service providers, which will also be subject to the "possession, custody, or control" test under a CLOUD Act request. These vendors likely meet the definition of "possession, custody, or control" because they can access and manipulate data stored by companies that use their services, even if their physical operations and servers are outside the U.S.

Providers have already begun strategically selecting vendors based on where they are located, as well as ensuring their compliance with the CLOUD Act, GDPR, and other relevant laws. Additionally, providers that use a single cloud vendor for all of their data storage needs will need to seek out different vendors in various jurisdictions to ensure compliance with applicable laws.[57] Foreign companies with U.S. subsidiaries may also try to limit their exposure to CLOUD Act requests by enforcing stricter segregation between U.S. and non-U.S. customers' data sets, so that information does not fall within the U.S. subsidiaries' "possession, custody, or control." Finally, companies may choose to encrypt much of the data that is subject to their "possession, custody, or control" in order to technically comply with CLOUD Act orders while keeping their customers' data out of the grasp of law enforcement officials.

56 Jonathan E. Meyer, *Foreign Companies: Does the U.S. Government Now Have Access to Your Overseas Data?*, National Law Review (Dec. 4, 2018), https://www.natlawreview.com/article/foreign-companies-does-us-government-now-have-access-to-your-overseas-data.

57 Michael Welts, *CLOUD Act: What Does That Mean For Your Cloud Storage*, Wasabi Blog (Aug. 31, 2018), https://wasabi.com/blog/cloud-act-mean-cloud-storage/.

Proponents of the CLOUD Act have pointed to the necessity of streamlining providers' obligations under conflicting foreign laws, since providers otherwise inevitably face sanctions for noncompliance with either one country's data request or another country's privacy laws.[58] Similarly, the EU's rationale for harmonizing the legal regime governing digital evidence-gathering is based on the fact that "the cost of complying with diverging national requirements, while presumably proportionate to market presence, can prove prohibitive to smaller providers."[59] Despite these positive intentions, companies will continue to face substantial costs and uncertainty about their obligations to fulfill requests for data, at least until a set of principles emerges for how to interpret and apply CLOUD Act requirements when served with QFG request. The U.S. executive branch may not be willing to set forth clear guidelines, and courts will have a very limited role in reviewing CLOUD Act requirements. As a result, how providers respond to their first-ever CLOUD Act requests will have a major effect on the future of data privacy in an increasingly interconnected legal regime where governments are no longer barred from legally obtaining data based on its physical location in the world.

Shelli Gimelstein *is a 2018 graduate of Stanford Law School. She writes on a variety of topics in privacy and technology law. Her work has been published in The University of Illinois Journal of Law, Technology & Policy and Stanford Law School Law & Policy Lab. She is a law clerk in the Intellectual Property Litigation group at a prominent law firm in New York City.*

58 CLOUD Act, H.R. 4943, 115th Cong. § 2 (2018).

59 *See* 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, *supra* note 30.