Stanford Law School

Riana Pfefferkorn
Associate Director of Surveillance
and Cybersecurity
Stanford Center for Internet
and Society
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
USA
+1 (650) 721-1491
riana@law.stanford.edu

November 13, 2018

Via E-Mail to pjcis@aph.gov.au, TOLAbill@aph.gov.au

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
Canberra ACT 2600
Australia

Re: Supplemental comments to Parliamentary Joint Committee on Intelligence & Security on the Telecommunication & Other Legislation Amendment (Assistance & Access) Bill 2018

To the Parliamentary Joint Committee on Intelligence and Security:

Thank you for inviting me to testify via videoconference before the Parliamentary Joint Committee on Intelligence and Security (PJCIS or the Committee) at its 16 November 2018 public hearing about the Telecommunication and Other Legislation Amendment (Assistance and Access) Bill 2018 (the Bill). I am the Associate Director of Surveillance and Cybersecurity at the Center for Internet and Society (CIS) at Stanford Law School in California. I make these comments, and will testify at the hearing, as a researcher who has studied encryption law and policy for the past three years. I appear in my personal capacity and do not represent Stanford University, Stanford Law School, or the Center for Internet and Society. My institutional affiliation is provided for identification purposes only.

I previously submitted written comments on the Bill on 9 September and 11 October 2018. In its invitation to testify on 16 November, the Committee indicated that it would welcome an additional submission in advance of the hearing and specifically requested my views on "the interaction between the US Clarifying Lawful Overseas Use of Data Act [CLOUD Act] and the Bill as proposed by government." This supplemental submission accordingly addresses the Committee's request. These comments pertain to the first-reading draft of the Bill of 20 September 2018[1] unless otherwise specified.

I. Background to the CLOUD Act

As you know, when Australian law enforcement authorities seek access to evidence held in the United States (or vice versa), they must go through the Mutual Legal Assistance Treaty (MLAT) process or another authorized procedure such as letters rogatory. The MLAT between Australia and the U.S. has been in effect since 1999.[2] Under the MLAT, an Australian law enforcement agency does not make a request directly

[1] As available in PDF at https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r6195_first-reps/toc_pdf/18204b01.pdf;fileType=application/pdf. Citations to page numbers refer to this PDF's numbering.
[2] A copy of the treaty is available online at http://www.austlii.edu.au/au/other/dfat/treaties/1999/19.html.

to the custodian of the evidence in the U.S.; rather, requests for assistance under the MLAT are handled by "Central Authorities" in each country. On the U.S. end, that means the Department of Justice (DOJ), which is headed by the Attorney General. In Australia, that means the Attorney-General or a minister designated by the Governor-General.

In recent years, as electronic evidence (such as e-mail, social media, and cloud storage accounts) proliferated and increasingly came to be held by large American tech companies, the MLAT process came under strain. Law enforcement authorities in other countries were stymied by months-long response times and by the need for requests to comply with the unfamiliar requirements of the federal Electronic Communications Privacy Act (ECPA). The ECPA regulates U.S. service providers' disclosure of information about their users. Prior to the CLOUD Act, it prohibited U.S. providers from disclosing users' metadata or communications content to foreign governments, full stop, "even if they [were] investigating their own citizens in connection with a local crime," which led "[t]hese blocking provisions [to be] an increasing source of frustration for foreign governments."[3]

At the same time, U.S. federal courts had rendered inconsistent decisions concerning U.S. law enforcement's authority under the federal Stored Communications Act (SCA), which is part of the ECPA, to compel U.S. service providers to produce the contents of user communications that were *not* located on servers in the U.S., but instead were either located on servers overseas or fragmented into "shards" spread across servers in multiple jurisdictions. The U.S. Supreme Court was considering a case addressing this issue (*United States v. Microsoft Corp.*) earlier this year, until the CLOUD Act's passage rendered the case moot.

The U.S. Congress's solution to these pressures on domestic and foreign law enforcement investigations was to pass the CLOUD Act in March of 2018. A copy of the legislative text as enacted is attached. The Act amends the ECPA to address both U.S. investigators' access to data held outside the U.S. and foreign investigators' access to data held inside the U.S. (The Committee's request for comment did not specify whether the former or the latter is of greater interest to the Committee, but given the focus of the Bill, these comments address the latter.)

The Act creates a path for qualifying foreign governments to essentially bypass the MLAT process, albeit only in matters of serious crime or terrorism.[4] It allows qualifying countries to enter a bilateral agreement with the U.S. that would remove some of the ECPA's blocking provisions and permit the country to serve electronic evidence demands directly on U.S.-based service providers rather than submitting requests through an intermediary like the U.S. DOJ. The hope is that this will streamline U.S. providers' compliance with foreign law enforcement requests.

For more information, I am attaching a copy of an April 2018 U.S. Congressional Research Service (CRS) report[5] about cross-border data sharing under the CLOUD Act.

II. CLOUD Act Requirements for Bilateral Agreement

Before a country can take advantage of the Act's MLAT bypass mechanism, it must first enter into a bilateral "executive agreement" with the U.S. The Act's provisions regarding executive agreements are codified at Section 2523 of Title 18 of the U.S. Code of federal statutes.

[3] Jennifer Daskal, "*Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0," *Stan. L. Rev. Online* (May 2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.
[4] Investigations that do not involve serious crime or terrorism offenses, or that are purely for intelligence purposes, would be ineligible for the CLOUD Act process. The Act does not define which offenses constitute "serious crime" besides terrorism.
[5] The CRS is the public-policy research arm of the U.S. Congress. It conducts nonpartisan research and analysis on national policy issues in response to congressional requests for information. Its reports are available online at https://crsreports.congress.gov/.

The Act imposes several requirements on these executive agreements (§ 2523(b)):

- *First*, a country can only qualify to enter an agreement if "the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement," as assessed by a number of factors (§ 2523(b)(1)).
- *Second*, the foreign country must have adopted appropriate data minimization procedures for information concerning U.S. persons "subject to the agreement" (§ 2523(b)(2)).
- *Third*, "the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data" (§ 2523(b)(3)).
- *Fourth*, the Act imposes certain requirements on any order subject to the agreement, some of which are discussed below (§ 2523(b)(4)).

Whether a proposed agreement satisfies these four conditions is to be determined by the U.S. Attorney General, with the concurrence of the U.S. Secretary of State (§ 2523(b)). The agreement is then submitted for review by the U.S. Congress, which has an opportunity to disapprove of that determination and preclude the agreement from coming into force (§ 2523(d)).

III. What the CLOUD Act Means for Australia

First off, it is important to bear in mind that Australian agencies will continue to have a legal channel for requesting data from U.S. service providers whether or not the U.S. and Australia ever enter a CLOUD Act agreement. That is because the Act does not replace other existing channels for requesting evidence, such as Australia's MLAT with the U.S. If the two countries never get around to negotiating an executive agreement,[6] the MLAT will still be in effect. If the United States decides that Australia does not qualify for a CLOUD Act agreement because its law does not adequately protect privacy and civil liberties (§ 2523(b)(1)), the MLAT will still be in effect. If an agreement is executed but is not renewed when it comes up for review after five years (§ 2523(e)), the MLAT will still be in effect. And during the lifetime of an agreement, if the U.S. government decides to "render the agreement inapplicable as to any order for which [it] concludes the agreement may not properly be invoked" (§ 2523(b)(4)(K)), then, again, the MLAT will still be in effect. That particular order would have to be refashioned into an MLAT request.

Previously, the MLAT and other authorized procedures such as letters rogatory were the only way for foreign governments to seek data from a U.S. provider. The CLOUD Act codifies executive agreements under the Act as a new possible alternative for qualifying governments. Outside of these mechanisms, there is no legal way under U.S. law for U.S. providers to respond to cross-border data requests from foreign governments—no matter what the foreign government's law purports to authorize. The passage of the CLOUD Act sets up a binary choice for foreign governments seeking evidence from U.S. providers: go through the MLAT (or letters rogatory) process, or go through the CLOUD Act agreement. Any extraterritoriality provisions in Australian law are not enough on their own.

The CLOUD Act reinforces the sovereignty of the United States in matters of cross-border evidence-gathering. The United States and Australia have already acknowledged that sovereignty by ratifying the Budapest Convention on Cybercrime.[7] That Convention expressly recognizes and enfranchises respect for

[6] To my knowledge, in the seven-plus months since the CLOUD Act passed, no country (including Australia) has entered an executive agreement with the U.S. *See* Peter Swire and Justin Hemmings, "Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act," *Lawfare* (Sept. 13, 2018), https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

[7] The text of the Convention is available at https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

sovereignty by acknowledging the need to establish and follow procedures for cross-border electronic evidence-gathering for criminal offenses.[8] As further discussed below, the CLOUD Act makes clear that providers and evidence located in the U.S. will be required to follow U.S. law, not foreign law, when it comes to cross-border data requests; a non-U.S. law enforcement agency may not simply order a U.S. provider to comply with its demand.

Unless and until Australia and the U.S. enter an executive agreement under the CLOUD Act, the status quo stands. The ECPA's blocking provisions continue to prohibit disclosure by U.S. providers to the Australian government, because those provisions cannot be lifted absent a CLOUD Act agreement. Australia must continue to submit all data requests through existing channels such as the MLAT.

If the Australian government wants to bypass the MLAT and serve data requests directly on U.S. providers, it must satisfy all of the CLOUD Act's requirements and go through the process of negotiating an executive agreement with the United States. The onus is on the Australian government to convince the United States that Australia meets all of the CLOUD Act's requirements.

If the two countries execute an agreement, every order the Australian government serves directly on a U.S. provider would also have to comply with the CLOUD Act's requirements. If a demand comports with Australian law but not with the terms of the agreement (which are dictated in part by the Act), the demand cannot be channeled through the agreement and Australia would have to fall back on the MLAT, letters rogatory, etc. If the demand does not fall within the scope of those mechanisms either, then there is no other means under U.S. law for the agency to obtain that data from the U.S. provider.

That is all true whether the Bill passes or not. The Bill cannot alter, abrogate, or supersede the CLOUD Act's requirements. If the Bill passes, Australia cannot bypass the MLAT process and serve demands under the Bill on U.S. providers without first entering a CLOUD Act agreement.

IV. Interaction of Certain CLOUD Act Requirements with the Bill

What, then, does the CLOUD Act mean for the Bill? As said, a CLOUD Act agreement must impose certain requirements on "any order that is subject to the agreement" (§ 2523(b)(4)). Failure to meet those requirements may result in the executive agreement's being deemed inapplicable to that order (§ 2523(b)(4)(K)).

As discussed below, parts of the Bill as presently drafted are (or could be implemented to be) incompatible with the Act's requirements. Therefore, despite the Bill's purpose of letting Australian investigative agencies seek assistance from foreign providers in investigations, the CLOUD Act would pose a barrier if an agency demand to a U.S. provider comports with the Bill but not with the Act.

What is more, "nothing in the CLOUD Act *authorizes* the foreign government to mandate disclosure" by the U.S. provider,[9] so an executive agreement under the Act would not guarantee that a U.S. provider would comply with a demand made under the Bill.

The Act's requirements for orders include, among others, the following three that I consider most pertinent to the Committee's inquiry: (1) requiring specific identifiers, (2) requiring the foreign country's law to supply the legal basis for the order, and (3) requiring independent judicial oversight.

[8] *See, e.g.*, Art. 25, ¶¶ 1, 4 ("The Parties shall afford one another mutual assistance to the widest extent possible … for the collection of evidence in electronic form of a criminal offence," "subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties"); Art. 27, ¶ 4(b) ("The requested Party may … refuse assistance if … it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests").

[9] David Bitkower and Natalie K. Orpett, "Congress Passes CLOUD Act Governing Cross-Border Law Enforcement Access to Data," Jenner & Block (2018), at p. 4, *available at* https://jenner.com/system/assets/publications/17847/original/CLOUD%20Client%20Alert%20_%20Congress%20Passes%20CLOUD%20Act%20Governing%20Cross-Border%20Law%20Enforcement%20Access%20to%20Data.pdf?1521851267.

1. **Specific identifier required in orders.** "[A]n order issued by the foreign government … shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order" (§ 2523(b)(4)(D)(ii)).

Interaction with the Bill: Section 317ZH's general limitations on TANs/TCNs purport to preclude notices from serving as stand-alone demands for private communications or user data without an underlying warrant or other relevant authorization (p. 52-54). The Explanatory Memorandum confirms "the need for a warrant or authorisation" (Explanatory Memorandum, p. 10). Typically, a warrant or authorization would be expected to specify a particular account, device, etc. However, the Bill's TAN and TCN provisions (§§ 317L, 317T) do not expressly require a TAN/TCN itself to be tied to a specific, identifiable "person, account, address, or personal device" or other identifier.

Any TAN or TCN the Australian government wishes to channel through the CLOUD Act agreement would have to include a specific identifier as required by the Act, *i.e.*, the specific account, device, etc. identified in the underlying warrant or other authorization. If a TAN or TCN fails to identify a specific identifier as the object of the notice, it cannot validly be served on a U.S. provider under a CLOUD Act agreement, irrespective of the Bill's intent for the notice to apply extraterritorially (§ 317ZH(2)(a), p. 53).

This portion of the CLOUD Act is intended to keep foreign countries from forcing U.S.-based providers to help them carry out mass surveillance. The U.S. DOJ has commented that this provision of the Act requires that orders "must be targeted at individual accounts. Bulk surveillance is not permitted."[10] That is just what some members of the public fear the Bill would allow. During the first Committee hearing on the Bill last month, two witnesses expressed concern that the Bill opens the door to mass surveillance,[11] a notion that representatives from the Home Affairs Office and ASIO denied.[12] Even assuming these fears are well-founded and this Bill will indeed enable mass surveillance by Australia of its own or other countries' citizens, the CLOUD Act is supposed to limit Australia's ability to dragoon U.S. providers into helping it do so.

What remains to be seen is whether the Act will be effective in that regard. As the Hon. Mark Dreyfus and a witness from the Communications Alliance pointed out during the October hearing, under current law, Australian telecommunications service providers and carriers already receive upwards of 300,000 warrantless requests per year from Australian law enforcement and intelligence agencies for the metadata of "specific individuals."[13] At that volume, "targeted" surveillance of individuals starts to look little different from "mass" or "bulk" surveillance, at least as the average Australian might understand those terms. The example of metadata demands to Australian telcos suggests that the CLOUD Act's "specific identifier" requirement would not, on its own, pose much of an obstacle to mass surveillance should the Bill pass. However, as discussed below, the CLOUD Act may pose other difficulties for Australian demands under the Bill.

---

[10] Remarks by Associate Attorney General Sujit Raman to the Center for Strategic and International Studies, Washington, D.C. (May 24, 2018), *available at* https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-center-strategic-and.

[11] Testimony of Mr. Patrick Fair, Communications Alliance (p. 41) (the Bill "has a massive impact on the ability of the agencies to do surveillance—and to do mass surveillance"), and Dr. Suelette Dreyfus, Blueprint for Free Speech (p. 55) ("this bill effectively opens the door, potentially, for mass surveillance by the state, depending on execution"), as transcribed in the Proof Committee Hansard, Parliamentary Joint Committee on Intelligence and Security, Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018, Canberra, ACT (Oct. 19, 2018), *available at* https://parlinfo.aph.gov.au/parlInfo/download/committees/commjnt/2a1771c8-f314-43f2-b9b0-cd09ad8123ae/toc_pdf/Parliamentary%20Joint%20Committee%20on%20Intelligence%20and%20Security_2018_10_19_6680.pdf;fileType=application%2Fpdf#search=%22committees/commjnt/2a1771c8-f314-43f2-b9b0-cd09ad8123ae/0000%22.

[12] Testimony of Messrs. Duncan Lewis, ASIO (pp. 2-3), and Michael Pezzullo, Department of Home Affairs (p. 7), as transcribed in the Proof Committee Hansard, *supra* n.11.

[13] Comments by the Hon. Mr. Dreyfus (p. 40) and Mr. John Stanton (p. 41), as transcribed in the Proof Committee Hansard, *supra* n.11.

2. **No stand-alone legal authority for orders.** "[A]n order issued by the foreign government … shall be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law" (§ 2523(b)(4)(D)(iii)). In addition, as noted, "the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data" (§ 2523(b)(3)).

Interaction with the Bill: The Act does not create any stand-alone legal authority for a foreign government to mandate any action by U.S. providers. It simply opens the door to allowing a U.S. provider, if a CLOUD Act executive agreement is in place, to disclose user data to Australia in response to an order from the Australian government that complies with the agreement, complies with Australian law, and does not require the provider to violate U.S. law. But it does not guarantee compliance with an Australian demand.

A CLOUD Act agreement could not enlarge the powers, or circumvent the limitations, of Australian agencies under Australian law. Thus, if the Bill passes, the Australian government could not validly issue an order to a U.S. provider under the CLOUD Act agreement except as authorized by the Bill (or other applicable Australian law).[14] As an example, the Australian government could not issue a CLOUD Act order to a U.S. provider to "implement or build a systemic weakness, or a systemic vulnerability, into a form of electronic protection," as the Bill expressly forbids that (§ 317ZG(1)(a), p. 52). That is, an Australian agency could not use a CLOUD Act agreement to achieve in the U.S. what it could not legally do in Australia.

Conversely, neither the CLOUD Act nor the Bill (nor the MLAT, for that matter) could force a U.S. provider to violate positive U.S. law. The Bill appears to recognize this general principle, at least as to TANs and TCNs (*see* § 317ZB(5), p. 43). However, U.S. law also implicates the "technical assistance requests" (TARs) that Schedule 1 of the Bill would create (§ 317G, pp. 17-19), as well as the voluntary disclosures of information contemplated in Schedule 5 of the Bill (§ 21A, p. 167-68). These Bill provisions are inconsistent with the ECPA's prohibitions against voluntary interceptions or disclosures of user data or communications content (18 U.S.C. §§ 2511(1)(c), 2702(a), 3121(a)).

As amended by the CLOUD Act, the ECPA now allows U.S. providers to disclose user data to qualifying foreign governments—but only in response to "an *order* from a foreign government that is subject to" a CLOUD Act executive agreement (18 U.S.C. §§ 2511(2)(j), 2702(b)(9), 2702(c)(7), 3121(a)) (emphasis added). A *request* to a U.S. provider for *voluntary* actions would be unenforceable; indeed, compliance would subject the U.S. provider to liability under the ECPA. More broadly, no matter what was requested (even if something other than the disclosure of user data or communications content in contravention of the ECPA), a mere request is not an "order" and is therefore invalid under the Act. In short, "compliance with the domestic law of" Australia is necessary but not sufficient for an Australian demand to a U.S. provider under a CLOUD Act agreement.

Even if an Australian demand complied with the terms of the CLOUD Act agreement and both U.S. and Australian law, the Act could not compel a U.S. provider's compliance with the demand. "Importantly, nothing in the CLOUD Act *authorizes* the foreign government to mandate disclosure. Rather, a CLOUD Act Agreement would permit the United States to remove barriers in existing American law that could prevent a US provider from complying with the foreign order."[15] "Although the CLOUD Act authorizes executive agreements that would remove ECPA's prohibitions on disclosure, neither the Act nor the agreements it authorizes create a legal obligation for service providers to comply with foreign governments' data demands. Rather, a foreign government's authority to issue an order seeking data must derive solely from its domestic law."[16]

[14] Nor could the Australian government use the executive agreement to order a U.S. provider to do something authorized by *U.S.* law, but not by Australian law.
[15] Bitkower and Orpett, *supra* n.9, at p. 4.
[16] Attached CRS report at p. 16 (footnotes omitted).

In other words, a CLOUD Act agreement would not *force* U.S. providers to comply with foreign demands. It would just lift the ECPA blocking provisions that currently *keep* them from complying. That is, a CLOUD Act agreement with a foreign government gives U.S. providers the *option*, but not the *obligation*, to comply with the foreign government's orders.

A CLOUD Act executive agreement with the U.S. should thus make it easier for Australian investigators to obtain the disclosure of, say, the contents of an e-mail account directly from a U.S. provider. Requests for metadata or the contents of communications (which many providers hold in a manner that allows disclosure in unencrypted form to law enforcement) are generally considered pretty run-of-the-mill by U.S. providers. Therefore, with a CLOUD Act agreement in place, U.S. providers might be likely to comply with orders to disclose user data that they already hold in unencrypted form—and without the long delays of the MLAT. Removing obstacles to compliance with such run-of-the-mill user data requests is the problem the CLOUD Act was intended to solve, and it might go a long way towards assuaging Australian agencies' presumable frustration with U.S. providers.

Where U.S. providers might balk at a foreign demand, and where the CLOUD Act would not force them to comply, is where the foreign government seeks to compel the provider to do something out of the ordinary that goes above and beyond what U.S. law requires. Accordingly, if the Bill passes, a CLOUD Act agreement could not force a U.S. provider to comply with an Australian demand to render technical assistance under a TAN or create or maintain a capability under a TCN. U.S. providers might be disinclined, even unable, to comply with a TAN/TCN. That is because the "listed acts or things" in Section 317E go beyond what U.S. federal law, the Communications Assistance for Law Enforcement Act (CALEA) of 1994, requires of U.S. providers.

As the name suggests, CALEA requires U.S. telecommunications carriers and equipment manufacturers to design their equipment, facilities, and services to guarantee law enforcement surveillance capabilities. Unlike the Bill, which has an extremely broad definition of "designated communications provider" (§ 317C), CALEA draws a legally-consequential distinction between "telecommunications carriers" and "information services" (47 U.S.C. § 1001(6), (8)). The former means, basically, the American equivalents of Telstra or Optus; the latter includes messaging apps (*e.g.*, WhatsApp), smartphone manufacturers (*e.g.*, Apple), social media platforms (*e.g.*, Facebook), e-mail providers (*e.g.*, Hotmail), and cloud storage providers (*e.g.*, Dropbox).

CALEA does not require information services to design their products and services to be accessible to law enforcement (47 U.S.C. § 1002(b)(2)). While it does impose access capability requirements on telecommunications carriers (47 U.S.C. § 1002(a)), it leaves carriers free to choose how to design their encryption offerings (47 U.S.C. § 1002(b)(3)). A carrier has no responsibility to decrypt encrypted communications for law enforcement unless the carrier provided the encryption and could in fact decrypt it (*id.*). In other words, CALEA does not prohibit a carrier from deploying an encryption service for which it does not retain the ability to decrypt communications for law enforcement access (*id.*). And CALEA does not limit information services' encryption deployment at all (*see id.*).

In short, in enacting CALEA, the U.S. Congress settled the question over 20 years ago of whether to mandate that U.S. providers of encrypted communications, devices, and storage services be able to decrypt encrypted data for law enforcement or provide technical assistance in decrypting.

Australia cannot implicitly compel through a CLOUD Act agreement what Congress expressly said U.S. law enforcement agencies cannot compel. Any executive agreement with Australia is flatly barred from "creat[ing] any obligation that providers be capable of decrypting data" (§ 2523(b)(3)). And the agreement cannot create its own stand-alone authority to mandate that U.S. providers do any other of the Bill's listed acts or things (§ 2523(b)(4)(D)(iii)).

Even if it could do so, Congress would have to explicitly amend CALEA to force U.S. carriers and information services to change their encryption designs. CALEA cannot be amended by an executive order or

executive agreement—that is, a CLOUD Act agreement could not singlehandedly change CALEA. Even if Congress allowed an agreement to come into force, that would not mean that CALEA was implicitly amended to require a foreign access solution. Congress would have to directly and expressly amend CALEA before any specific design or capability could be required of information services, or of telecommunications carriers beyond what CALEA currently requires. And amending CALEA is something Congress has not been willing to do. CALEA has never been amended in the 24 years since it was passed.

In sum, U.S. providers cannot be compelled under U.S. law to provide technical assistance or access to law enforcement of the kind contemplated by the Bill, and Australian law cannot change that. Whatever Australia's domestic law may be, and whatever extraterritorial reach it may claim to have, U.S.-based providers will decide whether or not to comply with Australian orders. For run-of-the-mill user data disclosure requests, they may well decide to comply. For technical assistance or capability notices, they may choose not to comply, and no CLOUD Act agreement can force them to. The providers will decide whether or not to manufacture their products and services specially for the Australian market, and will evaluate what risk there is to their employees or assets in Australia if the provider does not comply with Australian law. It is that business and risk analysis, not the CLOUD Act, that would dictate whether U.S.-based providers decide to comply with TANs, TCNs, or other orders Australia issued to them under the Bill.

3. **Independent judicial oversight of orders.** "[A]n order issued by the foreign government … shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order" (§ 2523(b)(4)(D)(v)).

Interaction with the Bill: As presently drafted, the Bill does not adequately provide for independent judicial oversight of TANs or TCNs. This shortcoming could render a CLOUD Act executive agreement inapplicable to TANs/TCNs to U.S. providers, whether or not the provider would be inclined to comply.

The Bill contains no requirement for prior independent review before the issuance of a TAN/TCN. Nor does the Bill provide for any independent review of third-party assessments as to whether a proposed TCN would violate Section 317ZG (*see* § 317W(7), p. 38). Post-issuance, the judiciary's only contemplated interaction with TANs/TCNs is Section 317ZFA's allowance for courts to "make such orders as the court considers appropriate in relation to the disclosure, protection, storage, handling or destruction, in the proceeding, of" TAN/TCN/TAR information, "if the court is satisfied that it is in the public interest to make such orders" (§ 317ZFA(1), p. 51). That is, once the notice has been issued, the provider has complied, and information thereby obtained by investigators has been introduced into evidence in court, the court may, if it so chooses, issue protective orders concerning the information.

That is not the same as making a TAN/TCN "subject to [judicial] review" as required by the CLOUD Act. As a public comment on the Bill from a coalition of over three dozen civil society groups, tech companies, and trade associations pointed out:

> the bill does not set forth any procedure to follow in challenging a technical assistance request, technical assistance notice, or technical capability notice, nor does it provide a clear and meaningful standard for a court to follow in reviewing such a challenge. … [T]he Explanatory Memorandum states that these notices are not subject to merits review (pp. 15, 29, 60). Moreover, given the bill's strict nondisclosure provisions …, "affected persons" will never know that a notice has been issued. Thus, even if companies receiving a notice might be able to challenge the demand as unlawful, the actual "affected persons" would not be able to do so. [¶] Finally, the bill fails to provide for any review or independent oversight of technical assistance notices or technical capability notices after they have been issued.[17]

[17] Comment by Coalition of Civil Society Organisations & Technology Companies & Trade Associations (Oct. 11, 2018) (Submission 29), p. 6. The Explanatory Memorandum referenced is available in PDF form at

The Bill and its Explanatory Memorandum do little to offset this critique. Section 317ZFA states that "[t]he powers conferred on a court by subsection (1) are in addition to any other powers of the court" (§ 317ZFA(2), p. 51), and the Explanatory Memorandum claims that "Australian courts will retain jurisdiction for judicial review of a decision" to issue a TAN or TCN, to "ensure that an affected person, or a provider o[n] behalf of an affected person, has an avenue to challenge unlawful decision making" (Explanatory Memorandum, § 45, p. 14). Compared to the serious shortcomings outlined above, these two short passages may carry little persuasive power in discussions with the U.S. about Australia's qualification for a CLOUD Act agreement.

Thus, absent significant amendments, there is a chance that the Bill's lack of independent judicial oversight for TANs and TCNs could be a sticking point if Australia seeks to qualify for a CLOUD Act agreement with the U.S. Even if Australia does qualify for and enter such an agreement, the lack of adequate independent oversight could render the agreement inapplicable to TANs and TCNs because they do not meet the CLOUD Act's judicial-oversight requirement (*see* § 2523(b)(4)(D)(v), (K)). That is, TANs and TCNs would be ineligible for direct service on U.S. providers.

That would leave official mechanisms such as the MLAT and letters rogatory. However, the MLAT has its own restrictions. It is my understanding (though I am not an MLAT expert) that the scope of the MLAT does not cover compelling a U.S. provider to provide technical assistance—it is simply a mechanism for cross-border data acquisition. Accordingly, it is my belief that TANs and TCNs would be out of scope of the MLAT.

In sum, with regard to the current version of the Bill, I believe TANs/TCNs are incompatible with the CLOUD Act and that neither the MLAT nor any prospective CLOUD Act agreement would supply a legal path for seeking a U.S. provider's response to a TAN/TCN.

V. Conclusion

I hope the above submission is helpful to the Committee. I look forward to the Committee's questions during the hearing on 16 November.

Sincerely,

Riana Pfefferkorn

Riana Pfefferkorn
Stanford Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
USA
Tel: +1 (650) 721-1491
Fax: +1 (650) 725-4086
riana@law.stanford.edu

https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf;fileType=application/pdf.

Attachment 1:

Text of CLOUD Act

DIVISION V—CLOUD ACT

SEC. 101. SHORT TITLE.

This division may be cited as the ''Clarifying Lawful Overseas Use of Data Act'' or the ''CLOUD Act''.

SEC. 102. CONGRESSIONAL FINDINGS.

Congress finds the following:

(1) Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism.

(2) Such efforts by the United States Government are being impeded by the inability to access data stored outside the United States that is in the custody, control, or possession of communications-service providers that are subject to jurisdiction of the United States.

(3) Foreign governments also increasingly seek access to electronic data held by communications-service providers in the United States for the purpose of combating serious crime.

(4) Communications-service providers face potential conflicting legal obligations when a foreign government orders production of electronic data that

United States law may prohibit providers from disclosing.

(5) Foreign law may create similarly conflicting legal obligations when chapter 121 of title 18, United States Code (commonly known as the ‘‘Stored Communications Act’’), requires disclosure of electronic data that foreign law prohibits communications-service providers from disclosing.

(6) International agreements provide a mechanism for resolving these potential conflicting legal obligations where the United States and the relevant foreign government share a common commitment to the rule of law and the protection of privacy and civil liberties.

SEC. 103. PRESERVATION OF RECORDS; COMITY ANALYSIS OF LEGAL PROCESS.

(a) REQUIRED PRESERVATION AND DISCLOSURE OF COMMUNICATIONS AND RECORDS.—

(1) AMENDMENT.—Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

‘‘§ 2713. Required preservation and disclosure of communications and records

‘‘A provider of electronic communication service or remote computing service shall comply with the obligations

of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.''.

(2) TABLE OF SECTIONS.—The table of sections for chapter 121 of title 18, United States Code, is amended by inserting after the item relating to section 2712 the following:

''2713. Required preservation and disclosure of communications and records.''.

(b) COMITY ANALYSIS OF LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—Section 2703 of title 18, United States Code, is amended by adding at the end the following:

''(h) COMITY ANALYSIS AND DISCLOSURE OF INFORMATION REGARDING LEGAL PROCESS SEEKING CONTENTS OF WIRE OR ELECTRONIC COMMUNICATION.—

''(1) DEFINITIONS.—In this subsection—

''(A) the term 'qualifying foreign government' means a foreign government—

''(i) with which the United States has an executive agreement that has entered into force under section 2523; and

"(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

"(B) the term 'United States person' has the meaning given the term in section 2523.

"(2) MOTIONS TO QUASH OR MODIFY.—(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes—

"(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

"(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

''(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that—

''(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

''(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

''(iii) the customer or subscriber is not a United States person and does not reside in the United States.

''(3) COMITY ANALYSIS.—For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate—

''(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

''(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

''(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

''(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

''(E) the nature and extent of the provider's ties to and presence in the United States;

''(F) the importance to the investigation of the information required to be disclosed;

''(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

''(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

''(4) DISCLOSURE OBLIGATIONS DURING PENDENCY OF CHALLENGE.—A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

''(5) DISCLOSURE TO QUALIFYING FOREIGN GOVERNMENT.—(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to

the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

''(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.''.

(c) RULE OF CONSTRUCTION.—Nothing in this section, or an amendment made by this section, shall be construed to modify or otherwise affect the common law standards governing the availability or application of comity analysis to other types of compulsory process or to instances of compulsory process issued under section 2703 of title 18, United States Code, as amended by this section, and not covered under subsection (h)(2) of such section 2703.

SEC. 104. ADDITIONAL AMENDMENTS TO CURRENT COMMUNICATIONS LAWS.

Title 18, United States Code, is amended—

(1) in chapter 119—

(A) in section 2511(2), by adding at the end the following:

''(j) It shall not be unlawful under this chapter for a provider of electronic communication service to the public or remote computing service to intercept or disclose the contents of a wire or electronic communication in response to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.''; and

(B) in section 2520(d), by amending paragraph (3) to read as follows:

''(3) a good faith determination that section 2511(3), 2511(2)(i), or 2511(2)(j) of this title permitted the conduct complained of;'';

(2) in chapter 121—

(A) in section 2702—

(i) in subsection (b)—

(I) in paragraph (8), by striking the period at the end and inserting ''; or''; and

(II) by adding at the end the following:

''(9) to a foreign government pursuant to an order from a foreign government that is subject to

an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.''; and

(ii) in subsection (c)—

(I) in paragraph (5), by striking ''or'' at the end;

(II) in paragraph (6), by striking the period at the end and inserting ''; or''; and

(III) by adding at the end the following:

''(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.''; and

(B) in section 2707(e), by amending paragraph (3) to read as follows:

''(3) a good faith determination that section 2511(3), section 2702(b)(9), or section 2702(c)(7) of this title permitted the conduct complained of;''; and

(3) in chapter 206—

(A) in section 3121(a), by inserting before the period at the end the following: ''or an

order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523''; and

(B) in section 3124—

(i) by amending subsection (d) to read as follows:

''(d) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with a court order under this chapter, request pursuant to section 3125 of this title, or an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.''; and

(ii) by amending subsection (e) to read as follows:

''(e) DEFENSE.—A good faith reliance on a court order under this chapter, a request pursuant to section 3125 of this title, a legislative authorization, a statutory authorization, or a good faith determination that the conduct complained of was permitted by an order from a for-

eign government that is subject to executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523, is a complete defense against any civil or criminal action brought under this chapter or any other law.''.

SEC. 105. EXECUTIVE AGREEMENTS ON ACCESS TO DATA BY FOREIGN GOVERNMENTS.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

''§ 2523. Executive agreements on access to data by foreign governments

''(a) DEFINITIONS.—In this section—

''(1) the term 'lawfully admitted for permanent residence' has the meaning given the term in section 101(a) of the Immigration and Nationality Act (8 U.S.C. 1101(a)); and

''(2) the term 'United States person' means a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation that is incorporated in the United States.

''(b) EXECUTIVE AGREEMENT REQUIREMENTS.—For purposes of this chapter, chapter 121, and chapter 206, an executive agreement governing access by a foreign government to data subject to this chapter, chapter 121, or chapter 206 shall be considered to satisfy the requirements of this section if the Attorney General, with the concurrence of the Secretary of State, determines, and submits a written certification of such determination to Congress, including a written certification and explanation of each consideration in paragraphs (1), (2), (3), and (4), that—

''(1) the domestic law of the foreign government, including the implementation of that law, affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement, if—

''(A) such a determination under this section takes into account, as appropriate, credible information and expert input; and

''(B) the factors to be met in making such a determination include whether the foreign government—

''(i) has adequate substantive and procedural laws on cybercrime and electronic

evidence, as demonstrated by being a party to the Convention on Cybercrime, done at Budapest November 23, 2001, and entered into force January 7, 2004, or through domestic laws that are consistent with definitions and the requirements set forth in chapters I and II of that Convention;

''(ii) demonstrates respect for the rule of law and principles of nondiscrimination;

''(iii) adheres to applicable international human rights obligations and commitments or demonstrates respect for international universal human rights, including—

''(I) protection from arbitrary and unlawful interference with privacy;

''(II) fair trial rights;

''(III) freedom of expression, association, and peaceful assembly;

''(IV) prohibitions on arbitrary arrest and detention; and

''(V) prohibitions against torture and cruel, inhuman, or degrading treatment or punishment;

''(iv) has clear legal mandates and procedures governing those entities of the foreign government that are authorized to seek data under the executive agreement, including procedures through which those authorities collect, retain, use, and share data, and effective oversight of these activities;

''(v) has sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data by the foreign government; and

''(vi) demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet;

''(2) the foreign government has adopted appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;

''(3) the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data; and

''(4) the agreement requires that, with respect to any order that is subject to the agreement—

''(A) the foreign government may not intentionally target a United States person or a person located in the United States, and shall adopt targeting procedures designed to meet this requirement;

''(B) the foreign government may not target a non-United States person located outside the United States if the purpose is to obtain information concerning a United States person or a person located in the United States;

''(C) the foreign government may not issue an order at the request of or to obtain information to provide to the United States Government or a third-party government, nor shall the foreign government be required to share any information produced with the United States Government or a third-party government;

''(D) an order issued by the foreign government—

''(i) shall be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;

''(ii) shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order;

''(iii) shall be in compliance with the domestic law of that country, and any obligation for a provider of an electronic communications service or a remote computing service to produce data shall derive solely from that law;

''(iv) shall be based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation;

''(v) shall be subject to review or oversight by a court, judge, magistrate, or other independent authority prior to, or in proceedings regarding, enforcement of the order; and

''(vi) in the case of an order for the interception of wire or electronic communications, and any extensions thereof, shall require that the interception order—

''(I) be for a fixed, limited duration; and

''(II) may not last longer than is reasonably necessary to accomplish the approved purposes of the order; and

''(III) be issued only if the same information could not reasonably be obtained by another less intrusive method;

''(E) an order issued by the foreign government may not be used to infringe freedom of speech;

''(F) the foreign government shall promptly review material collected pursuant to the agreement and store any unreviewed communications on a secure system accessible only to those persons trained in applicable procedures;

''(G) the foreign government shall, using procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), segregate, seal, or delete, and not disseminate material found not to be information that is, or is

necessary to understand or assess the importance of information that is, relevant to the prevention, detection, investigation, or prosecution of serious crime, including terrorism, or necessary to protect against a threat of death or serious bodily harm to any person;

''(H) the foreign government may not disseminate the content of a communication of a United States person to United States authorities unless the communication may be disseminated pursuant to subparagraph (G) and relates to significant harm, or the threat thereof, to the United States or United States persons, including crimes involving national security such as terrorism, significant violent crime, child exploitation, transnational organized crime, or significant financial fraud;

''(I) the foreign government shall afford reciprocal rights of data access, to include, where applicable, removing restrictions on communications service providers, including providers subject to United States jurisdiction, and thereby allow them to respond to valid legal process sought by a governmental entity (as defined in section 2711) if foreign law would oth-

erwise prohibit communications-service providers from disclosing the data;

"(J) the foreign government shall agree to periodic review of compliance by the foreign government with the terms of the agreement to be conducted by the United States Government; and

"(K) the United States Government shall reserve 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.

"(c) LIMITATION ON JUDICIAL REVIEW.—A determination or certification made by the Attorney General under subsection (b) shall not be subject to judicial or administrative review.

"(d) EFFECTIVE DATE OF CERTIFICATION.—

"(1) NOTICE.—Not later than 7 days after the date on which the Attorney General certifies an executive agreement under subsection (b), the Attorney General shall provide notice of the determination under subsection (b) and a copy of the executive agreement to Congress, including—

''(A) the Committee on the Judiciary and the Committee on Foreign Relations of the Senate; and

''(B) the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives.

''(2) ENTRY INTO FORCE.—An executive agreement that is determined and certified by the Attorney General to satisfy the requirements of this section shall enter into force not earlier than the date that is 180 days after the date on which notice is provided under paragraph (1), unless Congress enacts a joint resolution of disapproval in accordance with paragraph (4).

''(3) REQUESTS FOR INFORMATION.—Upon request by the Chairman or Ranking Member of a congressional committee described in paragraph (1), the head of an agency shall promptly furnish a summary of factors considered in determining that the foreign government satisfies the requirements of this section.

''(4) CONGRESSIONAL REVIEW.—

''(A) JOINT RESOLUTION DEFINED.—In this paragraph, the term 'joint resolution' means only a joint resolution—

"(i) introduced during the 180-day period described in paragraph (2);

"(ii) which does not have a preamble;

"(iii) the title of which is as follows: 'Joint resolution disapproving the executive agreement signed by the United States and ____.', the blank space being appropriately filled in; and

"(iv) the matter after the resolving clause of which is as follows: 'That Congress disapproves the executive agreement governing access by _____ to certain electronic data as submitted by the Attorney General on _____', the blank spaces being appropriately filled in.

"(B) JOINT RESOLUTION ENACTED.—Notwithstanding any other provision of this section, if not later than 180 days after the date on which notice is provided to Congress under paragraph (1), there is enacted into law a joint resolution disapproving of an executive agreement under this section, the executive agreement shall not enter into force.

''(C) INTRODUCTION.—During the 180-day period described in subparagraph (B), a joint resolution of disapproval may be introduced—

''(i) in the House of Representatives, by the majority leader or the minority leader; and

''(ii) in the Senate, by the majority leader (or the majority leader's designee) or the minority leader (or the minority leader's designee).

''(5) FLOOR CONSIDERATION IN HOUSE OF REPRESENTATIVES.—If a committee of the House of Representatives to which a joint resolution of disapproval has been referred has not reported the joint resolution within 120 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

''(6) CONSIDERATION IN THE SENATE.—

''(A) COMMITTEE REFERRAL.—A joint resolution of disapproval introduced in the Senate shall be referred jointly—

''(i) to the Committee on the Judiciary; and

''(ii) to the Committee on Foreign Relations.

"(B) REPORTING AND DISCHARGE.—If a committee to which a joint resolution of disapproval was referred has not reported the joint resolution within 120 days after the date of referral of the joint resolution, that committee shall be discharged from further consideration of the joint resolution and the joint resolution shall be placed on the appropriate calendar.

"(C) PROCEEDING TO CONSIDERATION.—It is in order at any time after both the Committee on the Judiciary and the Committee on Foreign Relations report a joint resolution of disapproval to the Senate or have been discharged from consideration of such a joint resolution (even though a previous motion to the same effect has been disagreed to) to move to proceed to the consideration of the joint resolution, and all points of order against the joint resolution (and against consideration of the joint resolution) are waived. The motion is not debatable or subject to a motion to postpone. A motion to reconsider the vote by which the motion is agreed to or disagreed to shall not be in order.

"(D) CONSIDERATION IN THE SENATE.—In the Senate, consideration of the joint resolution, and on all debatable motions and appeals in connection therewith, shall be limited to not more than 10 hours, which shall be divided equally between those favoring and those opposing the joint resolution. A motion further to limit debate is in order and not debatable. An amendment to, or a motion to postpone, or a motion to proceed to the consideration of other business, or a motion to recommit the joint resolution is not in order.

"(E) CONSIDERATION OF VETO MESSAGES.—Debate in the Senate of any veto message with respect to a joint resolution of disapproval, including all debatable motions and appeals in connection with the joint resolution, shall be limited to 10 hours, to be equally divided between, and controlled by, the majority leader and the minority leader or their designees.

"(7) RULES RELATING TO SENATE AND HOUSE OF REPRESENTATIVES.—

"(A) TREATMENT OF SENATE JOINT RESOLUTION IN HOUSE.—In the House of Rep-

resentatives, the following procedures shall apply to a joint resolution of disapproval received from the Senate (unless the House has already passed a joint resolution relating to the same proposed action):

''(i) The joint resolution shall be referred to the appropriate committees.

''(ii) If a committee to which a joint resolution has been referred has not reported the joint resolution within 7 days after the date of referral, that committee shall be discharged from further consideration of the joint resolution.

''(iii) Beginning on the third legislative day after each committee to which a joint resolution has been referred reports the joint resolution to the House or has been discharged from further consideration thereof, it shall be in order to move to proceed to consider the joint resolution in the House. All points of order against the motion are waived. Such a motion shall not be in order after the House has disposed of a motion to proceed on the joint resolution. The previous question shall be considered

as ordered on the motion to its adoption without intervening motion. The motion shall not be debatable. A motion to reconsider the vote by which the motion is disposed of shall not be in order.

''(iv) The joint resolution shall be considered as read. All points of order against the joint resolution and against its consideration are waived. The previous question shall be considered as ordered on the joint resolution to final passage without intervening motion except 2 hours of debate equally divided and controlled by the sponsor of the joint resolution (or a designee) and an opponent. A motion to reconsider the vote on passage of the joint resolution shall not be in order.

''(B) TREATMENT OF HOUSE JOINT RESOLUTION IN SENATE.—

''(i) If, before the passage by the Senate of a joint resolution of disapproval, the Senate receives an identical joint resolution from the House of Representatives, the following procedures shall apply:

"(I) That joint resolution shall not be referred to a committee.

"(II) With respect to that joint resolution—

"(aa) the procedure in the Senate shall be the same as if no joint resolution had been received from the House of Representatives; but

"(bb) the vote on passage shall be on the joint resolution from the House of Representatives.

"(ii) If, following passage of a joint resolution of disapproval in the Senate, the Senate receives an identical joint resolution from the House of Representatives, that joint resolution shall be placed on the appropriate Senate calendar.

"(iii) If a joint resolution of disapproval is received from the House, and no companion joint resolution has been introduced in the Senate, the Senate procedures under this subsection shall apply to the House joint resolution.

''(C) APPLICATION TO REVENUE MEASURES.—The provisions of this paragraph shall not apply in the House of Representatives to a joint resolution of disapproval that is a revenue measure.

''(8) RULES OF HOUSE OF REPRESENTATIVES AND SENATE.—This subsection is enacted by Congress—

''(A) as an exercise of the rulemaking power of the Senate and the House of Representatives, respectively, and as such is deemed a part of the rules of each House, respectively, and supersedes other rules only to the extent that it is inconsistent with such rules; and

''(B) with full recognition of the constitutional right of either House to change the rules (so far as relating to the procedure of that House) at any time, in the same manner, and to the same extent as in the case of any other rule of that House.

''(e) RENEWAL OF DETERMINATION.—

''(1) IN GENERAL.—The Attorney General, with the concurrence of the Secretary of State, shall review and may renew a determination under subsection (b) every 5 years.

''(2) REPORT.—Upon renewing a determination under subsection (b), the Attorney General shall file a report with the Committee on the Judiciary and the Committee on Foreign Relations of the Senate and the Committee on the Judiciary and the Committee on Foreign Affairs of the House of Representatives describing—

''(A) the reasons for the renewal;

''(B) any substantive changes to the agreement or to the relevant laws or procedures of the foreign government since the original determination or, in the case of a second or subsequent renewal, since the last renewal; and

''(C) how the agreement has been implemented and what problems or controversies, if any, have arisen as a result of the agreement or its implementation.

''(3) NONRENEWAL.—If a determination is not renewed under paragraph (1), the agreement shall no longer be considered to satisfy the requirements of this section.

''(f) REVISIONS TO AGREEMENT.—A revision to an agreement under this section shall be treated as a new agreement for purposes of this section and shall be subject to the certification requirement under subsection (b), and

to the procedures under subsection (d), except that for purposes of a revision to an agreement—

"(1) the applicable time period under paragraphs (2), (4)(A)(i), (4)(B), and (4)(C) of subsection (d) shall be 90 days after the date notice is provided under subsection (d)(1); and

"(2) the applicable time period under paragraphs (5) and (6)(B) of subsection (d) shall be 60 days after the date notice is provided under subsection (d)(1).

"(g) PUBLICATION.—Any determination or certification under subsection (b) regarding an executive agreement under this section, including any termination or renewal of such an agreement, shall be published in the Federal Register as soon as is reasonably practicable.

"(h) MINIMIZATION PROCEDURES.—A United States authority that receives the content of a communication described in subsection (b)(4)(H) from a foreign government in accordance with an executive agreement under this section shall use procedures that, to the maximum extent possible, meet the definition of minimization procedures in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801) to appropriately protect nonpublicly available information concerning United States persons.".

(b) TABLE OF SECTIONS AMENDMENT.—The table of sections for chapter 119 of title 18, United States Code, is amended by inserting after the item relating to section 2522 the following:

"2523. Executive agreements on access to data by foreign governments.".

SEC. 106. RULE OF CONSTRUCTION.

Nothing in this division, or the amendments made by this division, shall be construed to preclude any foreign authority from obtaining assistance in a criminal investigation or prosecution pursuant to section 3512 of title 18, United States Code, section 1782 of title 28, United States Code, or as otherwise provided by law.

☒

Attachment 2:

CRS Report on CLOUD Act

Cross-Border Data Sharing Under the CLOUD Act

Stephen P. Mulligan
Legislative Attorney

April 23, 2018

Congressional Research Service
7-5700
www.crs.gov
R45173

CRS REPORT
Prepared for Members and
Committees of Congress

Summary

Law enforcement officials in the United States and abroad increasingly seek access to electronic communications, such as emails and social media posts, stored on servers and in data centers in foreign countries. Because the architecture of the internet allows technology companies to store data at a great distance from the physical location of their customers, electronic communications that could serve as evidence of a crime often are not housed in the same country where the crime occurred. This disconnect has caused governments around the world, including the United States, to seek data stored outside their territorial jurisdictions. In the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Congress enacted one of the first major changes in years to U.S. law governing cross-border access to electronic communications held by private companies.

The CLOUD Act has two major components. The first facet addresses the U.S. government's ability to compel technology companies to disclose the contents of electronic communications stored on the companies' servers and data centers overseas. The Stored Communications Act (SCA) mandates that certain technology companies disclose the contents of electronic communications pursuant to warrants issued by U.S. courts based on probable cause that the communications contain evidence of a crime. But a dispute arose over whether warrants issued under the SCA could compel disclosure of data held outside the territorial jurisdiction of the United States. While the Supreme Court was set to resolve this issue in *United States v. Microsoft*, the CLOUD Act amended the SCA to require that technology companies provide data in their possession, custody, or control in response to an SCA warrant—regardless of whether the data is located in the United States. On April 17, 2018, the Supreme Court ruled that the change in law mooted the *Microsoft* case.

The second facet of the CLOUD Act addresses the reciprocal issue of foreign governments' ability to access data in the United States as part of their investigation and prosecution of crimes. Prior to the CLOUD Act, foreign nations seeking data in the United States were required to request the assistance of the U.S. government through either mutual legal assistance treaties (MLATs) or judicial instruments known as letters rogatory. Requests under either instrument are reviewed by U.S. courts before disclosure to the foreign nation can be authorized, but U.S. and foreign officials criticized the processes as inefficient and unable to accommodate the increasing number of data requests in the digital era.

The CLOUD Act responds to calls for modernization by authorizing the executive branch to conclude a new form of international agreement through which select foreign governments can seek data directly from U.S. technology companies without individualized review by the U.S. government. Agreements authorized by the CLOUD Act would remove legal restrictions on certain foreign nations' ability to seek data directly from U.S. providers in cases involving "serious crimes" when not targeting U.S. persons, provided the Executive has determined that the foreign nation's laws adequately protect privacy and civil liberties, among other requirements. While the CLOUD Act conditions approval of covered agreements upon a host of restrictions, commentators debate whether these agreements will provide adequate protections for privacy, human rights, and civil liberties.

Contents

Figures

Contacts

Law enforcement officials in the United States and abroad increasingly seek access to electronic communications, such as emails and social media posts, stored on servers and in data centers located in foreign countries.[1] The architecture of the internet allows technology companies significant flexibility as to the geographic location where they may store collected data.[2] As a result, electronic communications that may be evidence of a crime are not necessarily housed in the same country where the crime occurred.[3] This disconnect has caused governments around the world, including the United States, to seek data stored outside their territorial jurisdictions in the course of law enforcement investigations.[4] It also has led to debate over the extent to which national governments can compel private companies to disclose data stored in foreign nations and the degree to which civil liberties and privacy concerns should inform the proper procedure for sharing such data.[5]

In the United States, this debate largely has centered on the Stored Communications Act (SCA),[6] which is part of the broader Electronic Communications Privacy Act (ECPA).[7] Although the SCA generally prohibits certain technology companies from disclosing the contents of electronic communications to third parties,[8] it mandates disclosure to the U.S. government pursuant to a warrant based on probable cause that the communications contain evidence of a crime.[9] In *United States v. Microsoft Corp.*, the Supreme Court was set to address whether the United States could

[1] *See, e.g.*, Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 742-45 (2016) (analyzing trends of increased government demands for data located outside a nation's territorial jurisdiction); *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 1 (2017) [hereinafter *Data Stored Abroad Hearing*] (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen., U.S. Dep't of Justice), https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf [hereinafter Downing Statement] (outlining challenges to U.S. and foreign government efforts to obtain data overseas).

[2] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2490-91 (2014) ("Cloud computing is the capacity of Internet-connected devices to display data stored on remove servers rather than on the device itself.");Woods, *supra* note 1, at 739 ("[O]ne of the greatest societal and technological shifts *In re*cent years has been the move from storing data on a local machine—such as a cell phone or computer—to storing that data remotely on faraway servers, which can be accessed by a network such as the Internet.").

[3] *See, e.g.*, *Data Stored Abroad Hearing*, *supra* note 1 (statement of Paddy McGuinness, Deputy Nat'l Sec. Advisor, U.K.), https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf [hereinafter McGuinness Statement] (discussing the need for U.K. law enforcement access to data stored in the United States); *Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests Before the H. Comm. on the Judiciary*, 114th Cong. 22, 57-59 (2016) [hereinafter *International Conflicts of Law Hearing*] (statement of Brad Smith, President and Chief Legal Officer, Microsoft Corp.) [hereinafter Smith Statement] (discussing French requests for data stored by Microsoft following a 2015 terrorist attack in Paris).

[4] *See supra* notes 1-3. *See also infra* § *United States v. Microsoft Corp*. and the CLOUD Act (discussing the United States efforts to obtain data in Ireland); *International Conflicts of Law Hearing*, *supra* note 3, at 17-18 (statement of David Bitkower, Principal Assistant Deputy Att'y Gen., U.S. Dep't of Justice) [hereinafter Bitkower Statement] (listing examples of evidence gathered from American technology companies that was critical to solving crimes overseas); Peter Swire et al., *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323, 327 (2016) (discussing "how the globalization of data is affecting even routine criminal investigations").

[5] *Compare, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 329 (2015) (contending that the unique nature of data and the "physical disconnect between the location of data and the location of its user" undermines traditional notions of territorial sovereignty), *with* Woods, *supra* note 1, at 756-63 (arguing that data is compatible with existing conceptions of sovereignty and jurisdiction). *See also infra* § Commentary on the CLOUD Act (discussing commentary regarding the extent to which cross-border data sharing regimes should provide safeguards for privacy, human rights, and civil liberties).

[6] *See* 18 U.S.C. §§ 2701-2712.

[7] *See* P.L. 99-508, 100 Stat. 1848 (1986).

[8] *See* 18 U.S.C. § 2702(a).

[9] *Id.* § 2703(a).

compel Microsoft to release emails housed in a data center in Ireland through a warrant issued under the SCA.[10] But less than one month after oral argument, Congress passed and the President signed into law the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) as part of the Consolidated Appropriations Act, 2018.[11] The CLOUD Act amends the SCA and requires service providers subject to the SCA[12] to release data in their possession, custody, or control in response to an SCA warrant—regardless of whether the data is located in the United States.[13] After the U.S. government obtained a new warrant for the emails held in Ireland under the authority of the CLOUD Act, the Supreme Court deemed *Microsoft* moot.[14]

A second facet of the CLOUD Act addresses the reciprocal issue of foreign governments' desire to access data in the United States as part of their investigation and prosecution of crimes.[15] Prior to the CLOUD Act, foreign nations seeking data in the United States generally were required to request the assistance of the U.S. government through either procedures established by mutual legal assistance treaties (MLATs) or judicial requests known as letters rogatory.[16] Requests under either instrument are reviewed by U.S. courts before disclosure to the foreign nation is authorized, but U.S. and foreign officials have criticized these processes as inefficient and unable to accommodate the increasing cross-border data demands in the digital era.[17]

The CLOUD Act responds to calls for modernization by authorizing the executive branch to conclude a new form of international agreement[18] through which select foreign governments can seek data directly from U.S. technology companies without undergoing individualized review by the U.S. government.[19] Agreements authorized by the CLOUD Act would remove legal restrictions on certain foreign nations' ability to seek data directly from U.S. providers in cases involving "serious crimes" when not targeting U.S. persons, provided that the United States has

[10] *See* No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam).

[11] *See* Consolidated Appropriations Act, 2018, P.L. 115-141, div. V [hereinafter CLOUD Act].

[12] As discussed in more detail below, the SCA applies to a provider of an "electronic communications service," defined in 18 U.S.C. § 2510(15), and a "remote computing service," defined in 18 U.S.C. § 2711(2). *See infra* Overview of ECPA and the SCA. Unless otherwise indicated, the terms "service providers" or "providers" in this report reference both entities covered by the SCA.

[13] CLOUD Act § 103 (adding 18 U.S.C. § 2713).

[14] *See* No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam) (vacating and remanding with instructions to dismiss as moot).

[15] *See* CLOUD Act § 102(3) (discussing foreign governments' need to "access electronic data held by communications-service providers in the United States" in the congressional findings). *See also infra* § Executive Agreements Authorized by the CLOUD Act.

[16] *See* T. MARKUS FUNK, MUTUAL LEGAL ASSISTANCE TREATIES AND LETTERS ROGATORY: A GUIDE FOR JUDGES 1 (Fed. J. Center 2014), https://www.fjc.gov/sites/default/files/2017/MLAT-LR-Guide-Funk-FJC-2014.pdf; Woods, *supra* note 1, at 748-49. While MLATs and letters rogatory have been the standard legal avenues for seeking cross-border data, some information can be provided through informal channels, such as cooperative exchange between investigators. *See* FUNK, *supra*, at 23.

[17] *See, e.g.*, PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS 227 (2013) [hereinafter PRESIDENT'S REVIEW GROUP] ("The MLAT process . . . is too slow and cumbersome."); Downing Statement, *supra* note 1, at 7 ("[T]he [mutual legal assistance] process can lack the requisite efficiency for time-sensitive investigations and other emergencies, making it an impractical alternative to SCA warrants in many cases."); McGuinness Statement, *supra* note 3 ("It is widely acknowledged that MLAT processes are too slow for rapidly developing counter terrorism and serious crime investigations.").

[18] As used in this report, the term "international agreement" is intended to be a blanket term that includes all agreements between the United States and foreign nations that are intended to be binding under international law. *Accord* RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW: TREATIES, TENTATIVE DRAFT NO. 2, § 102 cmt. a (2017).

[19] *See infra* § Executive Agreements Authorized by the CLOUD Act.

determined that the foreign nation's laws adequately protect privacy and civil liberties, among other requirements.[20]

This report reviews the development of cross-border data sharing laws in criminal matters in the United States.[21] It begins with an overview of ECPA and the SCA.[22] Next, the report discusses the questions raised in the *Microsoft* litigation and the impact of the CLOUD Act on those issues.[23] Finally, the report examines the new form of international agreements authorized by the CLOUD Act and the commentary on the benefits and drawbacks of the potential new international data sharing agreements.[24]

Overview of ECPA and the SCA

Enacted in 1986, ECPA is one of the primary federal laws regulating disclosure of electronic communications held by private entities.[25] ECPA is structured on three main titles. Title I, commonly referred to as the Wiretap Act, governs the interception of real-time wire, oral, or electronic communications.[26] Title II added a new chapter to the *United States Code* entitled "Stored Wire and Electronic Communications and Transactional Records Access," and generally is referred to as the Stored Communications Act or SCA.[27] The SCA applies to many forms of electronic communications and associated data, including emails;[28] text messages;[29] private messages, wall postings, and other comments made on or via social media sites;[30] and private YouTube videos.[31] Title III of ECPA regulates the use of a pen register, a device that allows users to capture the routing information associated with communications, such as telephone numbers dialed.[32] Each title in ECPA contains restrictions on the circumstances in which the relevant data can be used or disclosed.[33]

---

[20] *See id.*

[21] Because this report focuses on data sharing in the context of criminal investigations, it does not address other, unrelated forms of information sharing, such as information sharing within an industry or with the government following a cyberattack, see CRS In Focus IF10163, *Cybersecurity and Information Sharing*, by N. Eric Weiss, or information shared among private companies for commercial purposes, see *Facebook, Social Media Privacy, and the Use and Abuse of Data, Hearing Before the S. Comm. on Commerce, Science, and Transportation* 115th Cong. (Apr. 10, 2018).

[22] *See infra* § Overview of ECPA and the SCA. Although constitutional provisions such as the Fourth Amendment are relevant to government access to personal data as part of a criminal investigation, *see* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (holding that the government must obtain a warrant to access certain stored emails), the focus of this report is on statutory protections.

[23] *See infra* § *United States v. Microsoft Corp.* and the CLOUD Act.

[24] *See infra* § Executive Agreements Authorized by the CLOUD Act.

[25] *See* P.L. 99-508, 100 Stat. 1848 (1986).

[26] *See id.* tit. I, 100 Stat. at 1848-59 (codified in 18 U.S.C. §§ 2510-2521).

[27] *Id.* at 1860.

[28] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004), *cert denied* 543 U.S. 813 (2004).

[29] *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 901 (9th Cir. 2008), *rev'd on Fourth Amendment grounds sub nom.* Quon v. City of Ontario, 560 U.S. 746 (2010).

[30] *See* Crispin v. Christian Audigier, 717 F. Supp. 2d 965, 980, 989 (C.D. Cal. 2010).

[31] *See* Viacom Intern. Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008).

[32] P.L. 99-508, tit. III, 100 Stat. 1848, 1868-73 (codified in 18 U.S.C. §§ 3121-3127).

[33] *See* 18 U.S.C. §§ 2511(1), 2702; 3121. For additional analysis of ECPA and its provisions, see CRS Report R41733, *Privacy: An Overview of the Electronic Communications Privacy Act*, by Charles Doyle, and CRS Report R41734, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, by Charles Doyle.

As technology has evolved since ECPA's enactment in 1986, law enforcement has shifted its primary focus from the interception of live communications pursuant to the Wiretap Act to seeking the now-common forms of stored communications governed by the SCA.[34] But the SCA does not apply the same provisions to every communication or data that falls under its ambit. Rather, the scope of the SCA may be impacted by whether the law is applied to a provider of "electronic communication services" (ECS) or "remote computing services" (RCS).[35] Although some SCA requirements vary depending on the provider,[36] the act has two core components that apply to both forms of provider: (1) prohibitions on disclosure of certain data and (2) mandatory disclosure provisions.[37]

Prohibitions on Disclosure Under the SCA

The first facet of the SCA is a restriction on providers' ability to share customers' electronic communications and their related records and information. Restrictions differ depending on the data at issue.[38] For the *contents* of electronic communications (e.g., the body of an email), the SCA prohibits disclosure to "any person or entity," absent an exception, provided certain technical requirements are met.[39] The SCA also prohibits both categories of provider from disclosing a "record or other information pertaining to a subscriber to or customer of such service" to the U.S. government.[40] This prohibition, which concerns non-content information or "metadata," does not prohibit disclosure to private entities or foreign governments.[41] The SCA

[34] *See* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 394 (2014).

[35] *See* 18 U.S.C. § 2702(a)(1)-(2).

[36] A provider of ECS allows its customers "to send or receive wire or electronic communications." *Id.* § 2510(15). A provider of RCS provides "computer storage or processing services by means of an electronic communication system." *Id.* § 2711(2).

[37] *See infra* §§ Prohibitions on Disclosure Under the SCA; Mandatory Disclosure Under the SCA.

[38] *See* 18 U.S.C. § 2702.

[39] Providers of ECS may not disclose the contents of communication "while in electronic storage." *Id.* § 2702(a)(1). Providers of RCS may not disclose the contents of a communication that is "carried or maintained" by the service, provided two additional conditions are satisfied. *Id.* § 2702(a)(2). First, the communication must be maintained "on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." *Id.* § 2702(a)(2)(A). Second, the communication must be maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing." *Id.* § 2702(a)(2)(B).

[40] *Id.* § 2702(a)(3) ("a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity."). The SCA defines "government entity" as "a department or agency of the United States or any State or political subdivision thereof." *Id.* § 2711(4).

[41] *Id.* § 2702(c)(6). Other federal or state laws may prohibit disclosure of particular classes of non-content information to foreign governments or private entities even if the SCA does not. *See, e.g.*, *id.* § 2710 (restricting disclosure of "prerecorded video cassette tapes or similar audio visual materials"); 20 U.S.C. § 1232g(b) (restricting the disclosure of "education records" by education agencies or institutions that receive federal funds).

enumerates several exceptions to the prohibition on disclosure of both content[42] and non-content communications.[43]

Mandatory Disclosure Under the SCA

The second major component of the SCA is its rules that *require* providers to disclose customer communications and related records to the U.S. government.[44] The SCA establishes a tiered system with differing procedures and standards governing when the U.S. government can demand that providers divulge stored communications.[45] As described below, the SCA's standards for mandatory disclosure depend on a number of factors, including, among other things, the type of data sought; whether an ECS or RCS holds the data; the length of time the data has been stored; whether the data is content or non-content; and whether advanced notice has been given to the customer.[46] The multitude of relevant factors can make the determination of whether disclosure is mandatory a complex and fact-specific evaluation.[47]

At the highest level, the SCA requires the U.S. government to obtain a warrant if the government seeks access from an ECS provider to the *content* of a communication that has been in "electronic storage" for 180 days or less.[48] A warrant may be issued only if the U.S. government demonstrates probable cause that the communications sought establish evidence of a crime.[49] If

[42] Among other exceptions enumerated in 18 U.S.C. § 2702(b), providers may divulge the content of communications: to an addressee or intended recipient; as may be necessary incident to the rendition of the service or the protection of the rights of property of the provider of that service; or to the U.S. government, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay.

[43] Exceptions to the prohibition on disclosure of non-content data are listed in 18 U.S.C. § 2702(c). These exceptions include, among things, disclosure (1) with the lawful consent of the customer or subscriber; (2) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (3) to the U.S. government, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay; (4) to the National Center for Missing and Exploited Children; and (5) to any non-U.S.-government person or entity.

[44] *See* 18 U.S.C. § 2703.

[45] *See infra* notes 48-53.

[46] *See id.*

[47] For example, whether disclosure of email content is required may depend on, among other factors, the technical architecture of the email system and whether the intended recipient opened the email. *See* United States v. Weaver, 636 F. Supp. 2d 769, 771 (C.D. Ill. 2009) (discussing how the SCA's mandatory disclosure requirements differ when applied to a "web-based email system" as compared to other email systems); Orin K. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1220-24 (2004) (providing background on ECPA). (discussing the application of the SCA's mandatory disclosure provisions to various forms of email in transit and in storage).

[48] 18 U.S.C. § 2703(a). "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). The case law generally holds that a user-opened email stored solely on the email provider's server is not in "electronic storage." *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1077 (9th Cir. 2004) ("A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Penn. 2001) ("[M]essages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage'").

[49] *See* 18 U.S.C. § 2703(a) (requiring that any warrant issued under the SCA be "issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction"); FED. R. CRIM. P. 41(d)(1) ("[A] magistrate judge—or if authorized . . . a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device.").

the communication has been stored for longer than 180 days, or if it is being "held or maintained" by an RCS "solely for the purpose of providing storage or computer processing services," the government can use a subpoena or a court order under 18 U.S.C. § 2703(d), provided notice is given to the customer.[50] To obtain an order under this section—known as a Section 2703(d) order—the applicant must prove "specific and articulable facts, showing that there are reasonable grounds to believe that the contents of a[n] . . . electronic communication . . . are relevant and material to an ongoing criminal investigation."[51]

In addition to the content of communications, the SCA permits access to non-content information with a warrant, but the government also may use a subpoena or a Section 2703(d) order to provide the customer notice.[52] To access basic subscriber information, including the customer's name, address, phone number, length of service, and means of payment (including bank account numbers), the government may follow the more stringent requirements for obtaining a warrant or a Section 2703(d) order, but it also can use an administrative subpoena, which requires no prior authorization by a judicial officer or notice to the customer.[53]

United States v. Microsoft Corp. and the CLOUD Act

While the complexities of the SCA coupled with major changes in technology have led some to call for broad reforms to the law,[54] one discrete issue—the extraterritorial application of the SCA—became the subject of particular interest as a result of a 2016 federal appellate court decision.[55] As noted above, the SCA mandates that service providers disclose the content of electronic communications when the government obtains a warrant based on probable cause.[56] In 2013, federal law enforcement officials sought an SCA warrant requiring Microsoft to disclose all emails and other information associated with an account with one of its customers.[57] After finding that the United States demonstrated probable cause that the account was being used to further illegal drug trafficking, a United States magistrate judge issued a warrant requiring Microsoft to disclose the contents of an email account and all records or information associated with the account "[t]o the extent that the information . . . is within [Microsoft's] possession, custody, or control."[58]

Microsoft complied with the portion of the warrant seeking metadata about the user's account (e.g., the name, IP address, and telephone number associated with the account), which was stored in the United States, but it determined that the contents of the user's emails were held in a data center in Dublin, Ireland.[59] Microsoft stores its users' emails in one of its many data centers

[50] *See* 18 U.S.C. § 2703(a); § 2703(b)(1)(B).

[51] *Id.* § 2703(d).

[52] *See id.* § 2703(c).

[53] *See id.*

[54] *See, e.g.*, Kerr, *supra* note 34, at 376-78; Caroline Lynch, *ECPA Reform 2.0. Previewing the Debate in the 115th Congress*, LAWFARE (Jan. 30, 2017), https://www.lawfareblog.com/ecpa-reform-20-previewing-debate-115th-congress.

[55] *See* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 829 F.3d 197, 222 (2d Cir. 2016) [hereinafter Matter of Warrant], *vacated and remanded with instructions to dismiss*, United States v. Microsoft Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369 (U.S. Apr. 17, 2018) (per curiam).

[56] *See supra* § Mandatory Disclosure Under the SCA.

[57] *See* United States v. Microsoft Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369, slip. op. at 1 (U.S. Apr. 17, 2018) (per curiam).

[58] *Id.*

[59] *Matter of Warrant*, 829 F.3d at 204.

around the world—most often the one closest to where users state they are from when signing up for the email service.[60] Although Microsoft did not dispute that it had the ability to access the emails in Ireland using computers inside the United States, it declined to comply with the portion of the warrant seeking data stored overseas on the ground that the SCA's mandatory disclosure provisions did not apply extraterritorially.[61]

The district court initially overruled Microsoft's objections, and it held the company in civil contempt for failing to produce the emails.[62] But the U.S. Court of Appeals for the Second Circuit (Second Circuit) reversed those rulings in 2016.[63] Relying on the presumption established by the Supreme Court that U.S. laws do not have effect outside U.S. territorial jurisdiction unless the law specifies otherwise,[64] the Second Circuit held that the SCA does not authorize the seizure of emails stored exclusively on foreign servers.[65] The United States appealed the Second Circuit's decision, and the Supreme Court granted certiorari in 2017 in *United States v. Microsoft, Corp.*[66]—a widely followed case that drew attention and amici curie briefs from a range of groups including privacy advocates, law enforcement officials, Members of Congress, 34 U.S. states and territories, and several foreign nations.[67]

The Legislative Response to *Microsoft* in the CLOUD Act

While the *Microsoft* appeal was pending before the Supreme Court, officials from the Department of Justice (DOJ) sought a legislative response to the Second Circuit's ruling.[68] In a hearing before the House Committee on the Judiciary in June 2017,[69] DOJ representatives argued that the Second Circuit's decision "effectively hamstrung the ability of law enforcement" to obtain data stored by U.S. service providers abroad, creating a "tremendous problem" that caused "substantial harm to public safety."[70] Accordingly, DOJ proposed a draft bill that would amend

[60] *See* Matter of Warrant, 829 F.3d 197, 204-06 (2d Cir. 2016), *vacated and remanded with instructions to dismiss*, United States v. Microsoft Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369 (U.S. Apr. 17, 2018) (per curiam).

[61] *See id.* at 209.

[62] *Id.* at 205.

[63] *See id.* at 222.

[64] *See* RJR Nabisco, Inc. v. European Cmty., 136 S.Ct. 2090, 2101 (2016); Morrison v. Nat'l Australia Bank Ltd., 561 U.S. 247, 266 (2010).

[65] *See Matter of Warrant*, 829 F.3d at 222.

[66] United States v. Microsoft Corp., 138 S.Ct. 356 (2017) (mem. op.), *vacated and remanded with instructions to dismiss*, No. 17-2, 548 U.S. __, 2018 WL 1800369 (U.S. Apr. 17, 2018) (per curiam).

[67] Among the more than 30 amici curie briefs were briefs filed by privacy groups; former law enforcement, national security and intelligence officials; 34 U.S. states and territories; the United Kingdom; Ireland; the European Commission (on behalf of the European Union); the New Zealand Privacy Commissioner; two U.S. Senators; and three Members of the U.S. House of Representatives. For a collection of amici briefs filed in *Microsoft*, see United States v. Microsoft Corp., SCOTUSBLOG (last visited Apr. 19, 2018), http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/.

[68] *See* Legislation to Permit Secure and Privacy-Protected Access to Cross-border Electronic Data for Law Enforcement to Combat Serious Crime and Terrorism [hereinafter 2017 DOJ Proposed Legislation], *in* Downing Statement, *supra* note 1, at app. A. The 2017 DOJ proposal also contained language derived from draft legislation prepared by DOJ in 2016 that addresses authorization for data sharing executive agreements, discussed *infra* § Executive Agreements Authorized by the CLOUD Act. *See infra* note 174 (discussing the DOJ's legislative proposal in 2016).

[69] *See Data Stored Abroad Hearing*, *supra* note 1.

[70] Downing Statement, *supra* note 1, at 1. *See also* Letter from Samuel R. Ramer, Acting Assistant Att'y Gen., U.S. Dep't of Justice, to the Honorable Paul Ryan, Speaker, U.S. House of Representatives (May 24, 2017), https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf [hereinafter Ramer Letter] (continued...)

provisions in ECPA, including provisions in the SCA, to state expressly that a service provider must comply with the law's mandatory disclosure requirements when the data is in the provider's possession, custody, or control—regardless of whether the data is located inside the United States.[71] As described by DOJ, the proposal was intended to restore the "pre-*Microsoft* status quo when providers routinely complied" with SCA warrants for data stored abroad.[72]

In February 2018, identical bills—both titled the CLOUD Act—containing DOJ's proposed extraterritoriality provision were introduced in the House and Senate.[73] The CLOUD Act was included in the Consolidated Appropriations Act, 2018, which was passed by both chambers, and signed into law by the President on March 23, 2018.[74] As enacted, the CLOUD Act amends ECPA by, among other things, including the following extraterritoriality provision:

> A [provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.[75]

After the CLOUD Act's enactment, the United States obtained a new warrant seeking the emails at issue in its dispute with Microsoft under the authority of the new law.[76] Because both the United States and Microsoft agreed that the new warrant replaced the prior warrant, the Supreme Court concluded that the case had become moot, and vacated the lower court's rulings with instructions to dismiss.[77]

Resolving Conflicts with Foreign Law

In addition to defining the extraterritorial reach of the mandatory disclosure provisions in ECPA, including the SCA, the CLOUD Act contains provisions designed to resolve potential conflicts of law that could arise if the United States seeks data stored abroad when the law of a foreign country prohibits disclosure.[78] It does so by authorizing a provider to file a motion to quash or modify a data demand if

(...continued)

("Congress can address the ongoing and substantial damage to public safety caused by the *Microsoft* decision . . . .").

[71] 2017 DOJ Proposed Legislation, *supra* note 68, § 3(a).

[72] Ramer Letter, *supra* note 70, at 1.

[73] *See* H.R. 4943, 115th Cong. (2018); S. 2383, 115th Cong. (2018). The CLOUD Act, as introduced and later enacted into law, contains minor variations on DOJ's proposed extraterritorial provision by removing the reference to a "provider of . . . wire communications"—a term not used in ECPA. *Compare* 2017 DOJ Proposed Legislation, *supra* note 68, § 3(a), *with* CLOUD Act § 103(a)(1) (adding 18 U.S.C. § 2713). The CLOUD Act also added the comity analysis, discussed *infra* § Resolving Conflicts with Foreign Law, which was not in the 2017 DOJ proposal, and made certain changes to DOJ's proposed authorization for international data sharing agreements, discussed *infra* § Executive Agreements Authorized by the CLOUD Act.

[74] *See supra* note 11.

[75] CLOUD Act § 103(a)(1) (adding 18 U.S.C. § 2713).

[76] United States v. Microsoft Corp., No. 17-2, 548 U.S. __, 2018 WL 1800369, slip op. at 2 (U.S. Apr. 17, 2018) (per curiam).

[77] *Id.*

[78] CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)).

- the provider reasonably believes the target of the demand is not a U.S. person[79] and does not reside in the United States;
- the provider reasonably believes disclosure would create a material risk of violating a foreign nation's law; and
- the foreign nation whose law may be violated has a data sharing agreement with the United States authorized by the CLOUD Act (discussed in more detail below[80]).[81]

A court may grant the providers' motion to modify or quash a government demand for data upon finding that three conditions are met: (1) the required disclosure would violate foreign law; (2) the interests of justice dictate that the demand should be quashed or changed; and (3) the target is not a U.S. person and does not reside in the United States.[82] In determining whether the second condition is satisfied, courts must undertake a "comity analysis."[83] Comity—or respect for foreign sovereignty[84]— is a legal doctrine that, among other things, permits courts to excuse violations of U.S. law, or moderate the sanctions imposed for such violations, when the violations are compelled by a foreign nation's law.[85] Courts and commentators often have described the comity doctrine as vague and ill-defined,[86] but the CLOUD Act specifically enumerates the

[79] The CLOUD Act defines "United States person" as a citizen or national of the United States, an alien lawfully admitted for permanent residence, an unincorporated business association in which a substantial number of members are citizens or lawfully admitted permanent residents, or a corporation that is incorporated in the United States. *See* CLOUD Act § 105(a) (adding 18 U.S.C. § 2523(a)(2)).

[80] *See infra* § Executive Agreements Authorized by the CLOUD Act.

[81] CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)). The foreign nation must also provide reciprocal rights allowing providers to quash or modify data demands in the foreign nation. *See id.*

[82] *See id*.

[83] *See id*.

[84] The classic definition of comity in U.S. law is derived from *Hilton v. Guyot*, an 1895 Supreme Court decision:

> "Comity," in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience, and to the rights of its own citizens, or of other persons who are under the protection of its laws.

159 U.S. 113, 163–64 (1895). For additional background on the comity doctrine, see William S. Dodge, *International Comity in American Law*, 115 COLUM. L. REV. 2071 (2015).

[85] *See* RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW: JURISDICTION, TENTATIVE DRAFT No. 2, § 222 (2016) [Hereinafter FOURTH RESTATEMENT: JURISDICTION TD 2] ("To the extent permitted by statute, regulation, or procedural rule, U.S. courts have discretion to excuse violations of U.S. law . . . on the ground that the violations are compelled by another state's law, if: (a) the person in question appears likely to suffer severe sanctions for failing to comply with foreign law; and (b) the person in question had acted in good faith to avoid the conflict."); *id.* at § 222 reporters' n.10 (stating that the defense of foreign state compulsion "reflects the practice of states in the interests of comity."). *See also* Société Internationale v. Rogers, 357 U.S. 197, 211 (1958) (ordering lower court to devise less severe sanctions for failure to produce banking records when "the very fact of compliance by disclosure . . . will itself constitute the initial violation of Swiss laws"); Gucci Am., Inc. v. Weixing Li, 768 F.3d 138 (2d Cir. 2014) (directing the district court to "undertake a comity analysis" due to the "apparent conflict between the obligations set forth in [an American court's injunction] and applicable Chinese banking law"); *In re* Sealed Case, 825 F.2d 494, 498 (D.C. Cir. 1987) (reversing dismissal of a contempt order and noting that the "government concedes that it would be impossible for the bank to comply with the contempt order without violating the laws of country Y on country Y's soil), *cert denied sub nom*, Roe v. United States, 484 U.S. 963 (1987).

[86] *See, e.g.*, JP Morgan Chase Bank v. Altos Hornos de Mexico, S.A. de C.V., 412 F.3d 418, 423 (2d Cir. 2005) ("International comity . . . has never been well-defined."); Turner Entm't Co. v. Degeto Film GmbH, 25 F.3d 1512, 1518 (11th Cir. 1994) (describing "respect for the acts of our fellow sovereign nations" as a "rather vague concept referred to in American jurisprudence as international comity"); Anne-Marie Slaughter, *Court to Court*, 92 AM. J. INT'L

(continued...)

factors courts should consider when determining whether comity principles support quashing or modifying a data demand.[87]

Notably, however, the CLOUD Act's comity factors and statutory right to a file a motion to quash or modify apply only to nations with which the United States has a data sharing agreement, as discussed below.[88] For nations with no such agreement, the CLOUD Act preserves common law principles of comity.[89] Common law comity principles generally dictate that U.S. legal obligations can be avoided as a result of foreign law only when the person or entity in question acted in good faith to avoid the conflict, but there remains a likelihood of severe sanctions in the foreign nation for failure to comply with foreign law.[90] Ultimately, the comity analysis under either the CLOUD Act *or* common law principles is likely to be a highly fact-specific evaluation that depends on the specific circumstances of a demand for data stored overseas.

International Data Sharing After the CLOUD Act

In addition to expressly expanding the ability of the U.S. government to require service providers to release data stored outside the United States, the CLOUD Act addresses a reciprocal issue: limitations on foreign governments' ability to obtain data in the United States.[91] As internet-based communications have become commonplace, evidence of criminal conduct frequently is derived from data stored on servers located outside the territorial jurisdiction of the nation where the crime was committed.[92] Because technology companies headquartered in the United States hold a majority of the world's electronic communications on their servers, foreign governments frequently seek data held by U.S. companies.[93] At the same time, ECPA prohibits service

(...continued)

L. 708, 708 (1998) ("Comity . . . is a concept with almost as many meanings as sovereignty."); Joel R. Paul, *Comity in International Law*, 32 HARV. INT'L L.J. 1, 4 (1991) ("[D]espite ubiquitous invocation of the doctrine of comity, its meaning is surprisingly elusive.").

[87] The CLOUD Act lists seven factors that the court "shall take into account, as appropriate[,]" in its comity analysis: (A) the United States' interests; (B) the foreign governments' interests; (C) the likelihood, extent, nature and penalties that the provider or its employees could face under foreign law; (D) the location and nationality of the target of the demand, and the nature and extent of the target's connections with the United States and the foreign nation; (E) the nature and extent of the provider's ties to and presence in the United States; (F) the importance of the information to the investigation to be disclosed; (G) the ability to access the information through other means; and (H) the investigative interests of the foreign nation if the data is sought by the United States on behalf of a foreign nation. *See* CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)(3)).

[88] *See* CLOUD Act § 103(b) (adding 18 U.S.C. § 2703(h)). *See also* § Executive Agreements Authorized by the CLOUD Act.

[89] *See* CLOUD Act § 103(c).

[90] *See* FOURTH RESTATEMENT: JURISDICTION TD 2, § 222.

[91] *See* CLOUD Act §§ 104-105.

[92] *See supra* notes 1-3. *See also* Letter from Peter J. Kadzik, U.S. Ass't Att'y Gen., to the Hon. Joseph R. Biden, President, U.S. Senate (July 15, 2016), https://tinyurl.com/y7b7fhaw [hereinafter Kadzik Letter] ("Foreign governments investigating criminal activities abroad increasingly require access to electronic evidence from U.S. companies that provide electronic communications to millions of their citizens and residents. Such data is often stored or accessible only in the United States . . . .").

[93] *See* TIFFANY LIN AND MAILYN FIDLER, CROSS-BORDER DATA ACCESS REFORM: A PRIMER ON THE PROPOSED U.S.-U.K. AGREEMENT 2 (2017), https://dash.harvard.edu/bitstream/handle/1/33867385/2017-09_berklett.pdf?sequence=1 ("Tech companies in the U.S. hold a majority of electronic data, meaning U.K. police investigating a crime in London, for example, may need to access emails stored by a U.S.-based provider."); Woods, *supra* note 1, at 780 ("[T]he vast majority of the world's Internet users store their data with U.S. firms . . . ."); McGuinness Statement, *supra* note 3 ("Most communications services are operated by companies based in the United States.").

providers from disclosing the content of electronic communications directly to foreign governments absent a statutory exception or a warrant from a federal court.[94]

With ECPA acting as a "blocking statute" that prevents foreign governments from directly acquiring certain third-party data stored by private entities in the United States, foreign nations have sought the U.S. government's assistance in obtaining warrants that authorize disclosure.[95] Prior to the CLOUD Act, there were two common international legal processes for obtaining a warrant in the United States: letters rogatory requests and MLATs.[96]

Three Forms of Cross-Border Data Sharing

Letters Rogatory. Discretionary requests made between the courts of one country to the courts of another country that are available to governments and private litigants, which are generally seen as the least efficient and reliable method of obtaining evidence abroad.[97]

Mutual Legal Assistance Treaties (MLATs). Treaties providing streamlined processes for cross-border evidence sharing between governments in criminal cases, which are reviewed by DOJ and a federal court for compliance with U.S. law.[98]

CLOUD Act Agreements. Executive agreements removing legal restrictions on certain foreign nations' ability to seek data directly from U.S. providers in cases involving "serious crimes" when not targeting U.S. persons, provided that the United States has determined that the foreign nation's laws adequately protect privacy and civil liberties.[99]

Letters Rogatory

Letters rogatory are requests made by a court in one nation to the court of another nation seeking assistance in obtaining evidence located abroad.[100] Historically, letters rogatory were the principle mechanism for sharing evidence between nations.[101] Whereas MLATs and agreements authorized under the CLOUD Act generally are limited to government-to-government requests in criminal

[94] *See* 18 U.S.C. § 2702(a)(3).

[95] *See, e.g.*, Aldert Gidari, *The Cross-Border Data Fix: It's Not So Simple*, CENTER FOR INTERNET AND SOCIETY, STANFORD LAW SCHOOL (Jun. 16, 2017) ("[L]aw enforcement outside the U.S. can't get data for their legitimate investigations from U.S. providers because the Electronic Communications Privacy Act (ECPA) prohibits such disclosures; that is, ECPA is a classic blocking statute."); *Data Stored Abroad Hearing*, *supra* note 1 (statement of Richard Salgado, Dir. of Law Enforcement and Information Security, Google Inc.), https://judiciary.house.gov/wp-content/uploads/2017/06/Salgado-Testimony.pdf [hereinafter Salgado Statement] ("ECPA includes a broad, so-called 'blocking' provision that restricts the circumstances under which U.S. service providers may disclose the content of users' communications to foreign governments.").

[96] *See* FUNK, *supra* note 16, at 1.

[97] *See infra* § Letters Rogatory.

[98] *See infra* § Mutual Legal Assistance Treaties (MLATs).

[99] *See infra* § Executive Agreements Authorized by the CLOUD Act.

[100] *See* Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241, 248 n.2 (2004) ("[A] *letter rogatory* is the request by a domestic court to a foreign court to take evidence from a certain witness.") (emphasis in original) (quoting Harry Leroy Jones, *International Judicial Assistance: Procedural Chaos and A Program for Reform*, 62 YALE L.J. 515, 519 (1953)); US. Dep't of State, *Preparation of Letters Rogatory*, TRAVEL.STATE.GOV, https://travel.state.gov/content/travel/en/legal/travel-legal-considerations/internl-judicial-asst/obtaining-evidence/Preparation-Letters-Rogatory.html [hereinafter *Preparation of Letters Rogatory*] ("Letters rogatory are requests from courts in one country to the courts of another country requesting the performance of an act which, if done without the sanction of the foreign court, could constitute a violation of that country's sovereignty.").

[101] *See* Peter Swire & Justin D. Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANN. SURV. AM. L. 687, 695 (2017) ("[I]nternational information sharing continued to rely on principles of comity and letters rogatory up until 1977.").

cases (with some exceptions in early MLATs),[102] criminal defendants and private litigants in civil cases may request that U.S. courts issue letters rogatory.[103] Governments may also use letters rogatory to seek judicial assistance in obtaining evidence abroad when the United States does not have either an MLAT or a CLOUD Act agreement with a foreign nation.[104]

Letters rogatory are discretionary requests premised on principles of comity rather than an obligation under international law.[105] There is no legal obligation or guarantee that the country receiving the request will respond,[106] and the evidence sharing process has been described as time-consuming and unpredictable.[107] Consequently, letters rogatory are often seen as the least preferable method of obtaining evidence abroad.[108]

Mutual Legal Assistance Treaties (MLATs)

As investigations into complex, coordinated international crimes like money laundering and drug trafficking became more common in the 1970s, the United States and other nations began to enter into MLATs, which established standardized procedures for sharing of certain evidence across national boundaries in criminal matters.[109] MLATs are treaties—most often bilateral treaties—in

[102] While early MLATs entered by the United States allowed criminal defendants to obtain some discovery abroad, more recent treaties expressly state that they do not give rise to a private right to submit requests. *Compare, e.g.*, Mutual Legal Assistance Treaty, arts. 12.2, 18.5, U.S.-Switz., entered into force Jan. 23, 1977, 27 U.S.T. 2019 (permitting criminal defendants or their counsel to be present during the production of witnesses or evidence *In re*sponse to MLAT requests), *with* Agreement on Mutual Legal Assistance, art. 3.5, U.S.-E.U., entered into force Feb. 1, 2010, 43 I.L.M. 758 ("The Contracting Parties agree that this Agreement is intended solely for mutual legal assistance between the States concerned. The provisions of this Agreement shall not give rise to a right on the part of any private person to obtain, suppress, or exclude any evidence, or to impede the execution of a request, nor expand or limit rights otherwise available under domestic law."). *See also* L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem*, 26 BERKELEY J. INT'L L. 62, 84 (analyzing U.S. MLATs and concluding that all but the three earliest treaties contain clauses restricting defense access to the mutual legal assistance process).

[103] *See, e.g.*, Yonatan L. Moskowitz, *MLATs and the Trusted Nation Club: The Proper Cost of Membership*, 41 YALE J. INTL. L. ONLINE 1, 3 (2016); FUNK, *supra* note 16, at 17.

[104] *Preparation of Letters Rogatory*, *supra* note 100 ("Letters rogatory are the customary means of obtaining judicial assistance from overseas in the absence of a treaty or other agreement.").

[105] *See, e.g.*, *In re* Letters Rogatory from Tokyo Dist., Tokyo, Japan, 539 F.2d 1216, 1219 (9th Cir. 1976) ("[T]he district court is given discretion in determining whether letters rogatory should be honored."); *In re* Letters Rogatory Issued by Na'l Court of First Instance in Commercial Matters N. 23 of Fed. Capital of Argentinean Republic, 144 F.R.D. 272, 274 (E.D. Pa. 1992) ("Because this is a subpoena granted pursuant to Letters Rogatory, this Court has broad discretion to decide whether to honor requests for foreign assistance."); Swire & Hemmings, *supra* note 101, at 692 ("Letters rogatory rely on principles of comity, or respect for foreign sovereignty, rather than on an assertion that the jurisdiction seeking the evidence has a legal right to the evidence."); FUNK, *supra* note 16, at 5 (stating that the process for letters rogatory is "more time-consuming and unpredictable" than MLATs "because the enforcement of letters rogatory is a matter of comity between courts, rather than treaty-based").

[106] Funk, *supra* note 16, at 19.

[107] *See, e.g.*, Virginia M. Kendall & T. Markus Funk, *The Role of Mutual Legal Assistance Treaties in Obtaining Foreign Evidence*, 40 LITIG. 59, 59 (2014) (describing letters rogatory as "a far less efficient and reliable process" than MLATs); *Preparation of Letters Rogatory*, *supra* note 100 ("Letters rogatory are customarily transmitted via diplomatic channels, a time-consuming means of transmission.").

[108] *See, e.g.*, OFFICE OF THE UNITED STATES ATTORNEYS, CRIMINAL RESOURCE MANUAL § 276, https://www.justice.gov/usam/criminal-resource-manual-276-treaty-requests (describing the MLAT process as "generally faster and more reliable than letters rogatory"); FUNK, *supra* note 16, at 3 ("[P]rosecutors typically consider letters rogatory an option of last resort for accessing evidence abroad, to be exercised only when MLATs are not available"); Woods, *supra* note 1, at 748 (describing letters rogatory as "rarely used and extremely unreliable").

[109] The United States first signed an MLAT with Switzerland in 1973, which entered into force in 1977. *See* Treaty between the United States of America and the Swiss Confederation on Mutual Assistance in Criminal Matters, U.S.-
(continued...)

which nations agree to provide certain assistance to foreign governments in the investigation and prosecution of crimes.[110] Whereas letters rogatory are discretionary requests, MLATs create treaty-based obligations governed by international law.[111]

While the requirements in each MLAT may differ depending on the specific terms of the treaty, MLATs generally obligate nations to summon witnesses, compel the production of documents and other evidence, issue warrants, and serve process in response to requests from the foreign government.[112] MLATs typically also identify grounds for refusing requests.[113] The United States has MLATs with more than 60 nations,[114] but this accounts for less than half the nations in the world.[115]

Each party to an MLAT designates a central authority through which direct communications can be made.[116] The central authority for the United States is the Office of International Affairs (OIA)

(...continued)

Switz., May 25, 1973, 27 U.S.T. 2019, T.I.A.S. 8302. *See also Consular Conventions, Extradition Treaties, and Treaties Relating to Mutual Legal Assistance in Criminal Matters (MLATs): Hearing Before the S. Comm. on Foreign Relations*, 102d Cong. 1, 11 (1992) (statement of Robert S. Mueller, III, Assistant Att'y Gen., Criminal Div., U.S. Dep't of Justice) [hereinafter Mueller Statement] ("We concluded our first MLAT, with Switzerland, to facilitate access to Swiss bank records. Financial records are vital to the successful prosecution of organized crime bosses and drug kingpins, who are rarely caught red-handed . . . ."); Richardson, *supra* note 102, at 98 (providing background on the U.S.-Swiss MLAT).

[110] For a list of U.S. MLATs, see 2 U.S. DEP'T OF STATE, BUREAU FOR INT'L NARCOTICS AND LAW ENFORCEMENT AFFAIRS, INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT: MONEY LAUNDERING AND FINANCIAL CRIMES 21 (2014)[hereinafter STRATEGY REPORT] and 7 Foreign Affairs Manual (F.A.M.) § 962.1(d), https://fam.state.gov/FAM/07FAM/07FAM0960.html.

[111] *See In re* Commissioner's Subpoena, 325 F.3d 1287, 1292–1304 (11th Cir. 2003) (explaining that "[l]aw enforcement authorities found the statute" authorizing federal district courts to entertain letters rogatory "to be an unattractive option in practice because it provided wide discretion in the district court to refuse the request and did not obligate other nations to return the favor that it grants. MLATs, on the other hand, have the desired quality of compulsion as they contractually obligate the two countries to provide to each other evidence and other forms of assistance needed in criminal cases while streamlining and enhancing the effectiveness of the process for obtaining needed evidence."), *abrogated in part on other grounds by* Intel Corp. v. Advanced Micro Devices, Inc., 542 U.S. 241 (2004); Swire & Hemmings, *supra* note 101, at 695-96 (describing the development of comity-based requests to treaty-based requests).

[112] 7 F.A.M. § 962.1(a). *See also* FUNK, *supra* note 16, at 5 (listing common types of assistance in MLATs).

[113] *See, e.g.*, Treaty Between the United States and Ukraine on Mutual Legal Assistance in Criminal Matters, U.S.-Ukr., art. 3, entered into force Feb. 27, 2001, S. TREATY DOC. 106-16 (stating that the central authority of the requesting state may deny assistance if, among other reasons, the request relates to an offense under military law or would prejudice the "security or similar essential interests" of the receiving state).

[114] The United States has bilateral MLATs with more than 50 nations and is also a party to the multilateral Agreement on Mutual Legal Assistance with the European Union and the Inter-American Convention on Mutual Legal Assistance of the Organization of American States. *See* STRATEGY REPORT *supra* note 110, at 21. The United States is also a party to other multilateral treaties, such as the International Convention for the Suppression of the Financing of Terrorism, *opened for signature* Jan. 10, 2000, 2178 U.N.T.S. 197, and the United Nations Convention Against Corruption, *opened for signature* Dec. 9, 2003, 2349 U.N.T.S. 41, which provide for cooperation in the investigation and prosecution of the particular offenses that are the subject of the treaties. *See id*; RESTATEMENT (FOURTH) OF FOREIGN RELATIONS LAW: JURISDICTION, TENTATIVE DRAFT No. 3, § 313 reporters n.1 (2017).

[115] *See* U.S. Dep't of State, Bureau of Intelligence and Research, *Independent States in the World* (Jan. 20, 2017), https://www.state.gov/s/inr/rls/4250.htm (identifying 195 independent nations). *See also* Downing Statement, *supra* note 1, at 7 ("[T]he United States maintains bilateral MLA treaties with less than one-half of the world's countries.").

[116] 7 F.A.M. § 962.1(a); Mueller Statement, *supra* note 109, at 11 ("The most significant benefit of MLATs may lie in institutionalizing law enforcement cooperation . . . by mandating for each treaty partner a Central Authority which serves as the clearinghouse for all incoming and outgoing requests.").

in the Criminal Division of DOJ.[117] When a request for legal assistance is submitted to the United States,[118] OIA receives and conducts an initial review to ensure that the request contains all necessary information and comports with required formats.[119] OIA then transmits the request to the U.S. Attorney in the jurisdiction where the witness or evidence is located.[120] The U.S. Attorney brings the request before a federal district court by filing a request for a court order or warrant authorizing the United States to carry out the action sought by the foreign nation.[121] Before authorizing the action, courts review the request to ensure that it complies with the underlying treaty and U.S. law and constitutional requirements.[122] After a warrant or court order has been issued and the provider transfers the data to the U.S. government, OIA and the Federal Bureau of Investigation (FBI) review the material in an effort to minimize production of information that is not responsive to the request.[123]

According to the 2013 President's Review Group on Intelligence and Communications Technologies, MLAT requests submitted to the United States take an average of approximately 10 months to complete.[124] When the United States seeks data from foreign nations, some requests take "considerably longer,"[125] especially when submitted to countries that are uncooperative or have less sophisticated legal systems.[126] According to one U.S. official, the United States never receives a response to some requests.[127]

Executive Agreements Authorized by the CLOUD Act

Although the MLAT process generally is seen as more predictable and efficient than letters rogatory,[128] MLATs became the subject of criticism in recent years due to, among other things, the typical length of response time under such agreements and the fact that the United States does not

[117] 7 F.A.M. § 962.1(c).

[118] Outgoing MLAT requests from the United States to foreign nations often follow similar procedures as incoming requests, but the process depends on the nation receiving the request. *See* Bitkower Statement, *supra* note 4, at 21 (discussing the general procedure through which OIA serves MLAT requests on foreign nations); Swire et al., *supra* note 4, at 357 (detailing the process by which the United States submits MLAT requests to France).

[119] *See* Swire & Hemmings, *supra* note 101, at 698. For additional background the MLAT process, see FUNK, *supra* note 16, at 6-11.

[120] There are 93 U.S. Attorneys stationed throughout the United States and its territories, and each serves as the "chief federal law enforcement officer of the United States within his or her particular jurisdiction." U.S. Dep't of Justice, Office of the Attorney General, *Mission*, JUSTICE.GOV (last updated Sep. 22, 2016), https://www.justice.gov/usao/mission.

[121] *See* FUNK, *supra* note 16, at 6; Swire & Hemmings, *supra* note 101, at 699.

[122] *See In re* Dolours Price, 685 F.3d 1, 15 (1st Cir. 2012) ("It is undisputed that treaty obligations are subject to some constitutional limits."); *In re* Premises Located at 840 140th Avenue NE, Bellevue, Washington, 634 F.3d 557, 572 (9th Cir. 2011) ("At a minimum, the Constitution requires that a request not be honored if the sought-after information would be used in a foreign judicial proceeding that 'depart[s] from our concepts of fundamental due process and fairness.'") (quoting *In re* Request for Judicial Assistance from Seoul District Criminal Court, 555 F.2d 720, 724 (9th Cir. 1977)); FUNK, *supra* note 16, at 5 ("[T]he district court must still review the terms of each request, checking that they comply with the terms of the underlying treaty and comport with U.S. law.").

[123] *See* Swire & Hemmings, *supra* note 101, at 699.

[124] *See* PRESIDENT'S REVIEW GROUP, *supra* note 17, at 227.

[125] *See* Bitkower Statement, *supra* note 4, at 21.

[126] *Id*.

[127] *Id*.

[128] *See supra* note 107-108.

have any MLAT with more than half the nations in the world.[129] At the same time, the number of requests for assistance in obtaining data and other evidence in the United States has increased markedly. In its FY2017 budget request, DOJ stated that the number of requests for judicial assistance from foreign countries increased nearly 85%, and the number for requests for "computer records" increased over 1000%.[130]

As foreign governments' need for data located overseas has expanded, some nations have sought data directly from U.S. providers and passed legislation authorizing their governments to compel disclosure.[131] These developments have placed U.S. technology companies at the intersection of potentially conflicting legal obligations: service providers may be both subject to foreign court orders compelling the release of data and prohibited by U.S. law from disclosing that data.[132] The potentially conflicting obligations coupled with criticisms of the MLAT and letters rogatory processes led to proposals for changes in the international data sharing regime that ultimately culminated in the CLOUD Act.[133]

The CLOUD Act creates a third paradigm of international data sharing arrangements: the possibility of international agreements that remove legal restrictions on U.S. technology companies' ability to disclose data directly to certain foreign nations in response to "orders" issued by foreign nations.[134] Whereas MLATs are "treaties" within the meaning of U.S. constitutional law—meaning they are binding international agreements concluded by the Executive after receiving the advice and consent of the Senate as provided in the Treaty Clause[135]—the CLOUD Act authorizes the United States to enter "executive agreements" with qualifying foreign nations.[136] Executive agreements are binding international agreements entered

[129] *See*, *e.g.*, PRESIDENT'S REVIEW GROUP, *supra* note 17, at 227 (identifying problems with and proposing six steps to improve the MLAT process); Bitkower Statement, *supra* note 4, at 35-36; Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. FOR INTERNET AND SOC'Y, STANFORD LAW SCH. (Feb. 23, 2015), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained. *See also supra* note 114 (discussing the nations with which the U.S. has MLATs).

[130] CRIMINAL DIV., U.S. DEP'T OF JUSTICE, PERFORMANCE BUDGET: FY 2017 PRESIDENT'S BUDGET 23 (2016), http://www.justice.gov/jmd/file/820926/download.

[131] *See* Downing Statement, *supra* note 1, at 8. *See also* Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SEC. L. J. (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ (discussing foreign nations' desire to obtain data from U.S. companies through foreign subsidiaries).

[132] *See* Downing Statement, *supra* note 1, at 8 ("Our companies may face conflicting legal obligations when foreign governments require them to disclose electronic data in the United States that U.S. law prohibits them from disclosing"); Smith Statement, *supra* note 3, at 62 (describing conflicting legal obligations faced by Microsoft as result of Brazilian court orders compelling the disclosure of the contents of electronic communications stored outside Brazil).

[133] *See* CLOUD Act § 102 (including in congressional findings that "[t]imely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime," but that such access is "impeded by the inability to access data stored outside the United States[,]" and potentially subject to "conflicting legal obligations" under U.S. and foreign law).

[134] *See* CLOUD Act §§ 104-105.

[135] *See* U.S. CONST., art. II, § 2, cl. 2 ("The President . . . shall have Power, by and with the Advice and Consent of the Senate, to make Treaties, provided two thirds of the Senators present concur[.]"). The term "treaty" has a broader meaning under international law, in which it is generally synonymous with all binding agreements, than in the context of domestic law, in which it refers to the subcategory of international agreements that are concluded by the President after receiving the advice and consent of the Senate. *See* CRS Report RL32528, *International Law and Agreements: Their Effect upon U.S. Law*, by Michael John Garcia, at 2.

[136] CLOUD Act § 105.

into by the Executive based on a source of authority other than the Treaty Clause.[137] The Executive's authority often is derived from legislation, as is the case in the CLOUD Act.[138]

The executive agreements authorized under the CLOUD Act would allow service providers to disclose the contents of electronic communications—both stored communications and real-time communications intercepted by wiretap—directly to requesting foreign governments with whom the United States has an authorized data sharing agreement.[139] The Act does so by removing ECPA's prohibitions on disclosure to such foreign governments.[140] When a foreign nation with a CLOUD Act agreement issues an "order" seeking data from a provider in the United States, the provider can deliver the requested data without civil or criminal penalty under ECPA.[141] By contrast, in the MLAT and letters rogatory processes, cross-border data requests initially are submitted to government entities rather than to the private party in possession of the data.[142]

Although the CLOUD Act authorizes executive agreements that would remove ECPA's prohibitions on disclosure, neither the Act nor the agreements it authorizes create a legal obligation for service providers to comply with foreign governments' data demands.[143] Rather, a foreign government's authority to issue an order seeking data must derive solely from its domestic law.[144] Additionally, state or federal laws other than ECPA still may prohibit disclosure of particular classes of information.[145]

Requirements for CLOUD Act Agreements

The CLOUD Act contains a number of restrictions on the type of foreign governments with whom the United States can enter agreements and the nature of demands for data that qualifying foreign governments can issue to U.S. providers.[146] Before an agreement concluded under the CLOUD Act can enter into force, the Attorney General, with the concurrence of the Secretary of

[137] Although not mentioned expressly in the Constitution, the executive branch has entered into executive agreements on a variety of subjects without the advice and consent of the Senate since the early years of the Republic. *See, e.g.*, Am. Ins. Ass'n v. Garamendi, 539 U.S. 396, 415 (2003) ("[O]ur cases have recognized that the President has authority to make 'executive agreements with other countries, requiring no ratification by the Senate . . . this power having been exercised since the early years of the Republic"); L. HENKIN, FOREIGN AFFAIRS AND THE UNITED STATES CONSTITUTION 219 (2d ed. 1996) ("Presidents . . . have made many thousands of [executive] agreements, differing in formality and importance, on matters running the gamut of U.S. foreign relations."). For additional background on the difference between treaties and executive agreements, see CRS Report RL32528, *supra* note 135, at 2-9.

[138] Executive agreements that are authorized by legislation enacted through the bicameral process are known as "congressional-executive" agreements. *See* CRS Report RL32528, *supra* note 135, at 5.

[139] *See* CLOUD Act § 104.

[140] The CLOUD Act amends portions of the Wiretap Act (18 U.S.C. §§ 2511(2), 2520(d)), the SCA (*id*. § 2702(b)-(c)), and the Pen Register Statute (*id*. §§ 3121(a), 3124(d)) by permitting disclosure pursuant to an executive agreement authorized by the Act. *See* CLOUD Act § 104.

[141] In addition to removing prohibitions in the Wiretap Act, SCA, and Pen Register statute, *supra* note 140, the CLOUD Act amends each act to make a good faith belief that disclosure was permitted pursuant to an executive agreement a defense to liability. *See* CLOUD Act § 104.

[142] *See supra* §§ Letters Rogatory; Mutual Legal Assistance Treaties (MLATs).

[143] CLOUD Act § 105 (requiring that "any obligation for a provider of electronic communications service or remote computing service to produce data" under a CLOUD Act agreement "shall derive solely" from the foreign nation's law).

[144] *Id.*

[145] *See, e.g.*, 12 U.S.C. § 3402 (providing "no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless" statutory exceptions apply); 18 U.S.C. § 2710 (restricting disclosure of "prerecorded video cassette tapes or similar audio visual materials").

[146] *See* CLOUD Act § 105.

State, must make four written certifications that are provided to Congress and published in the *Federal Register*:

1. the foreign nation's domestic law "affords robust substantive and procedural protections for privacy and civil liberties" in its data-collection activities, as determined based on at least seven statutory factors;[147]
2. the foreign government has adopted "appropriate" procedures to minimize the acquisition, retention, and dissemination of information concerning U.S. persons;
3. the executive agreement will not create an obligation that providers be capable of decrypting data, nor will it create a limitation that prevents providers from decryption;[148] and
4. the executive agreement will require that any order issued under its terms will be subject to an additional set of procedural and substantive requirements, as discussed below.[149]

The CLOUD Act expressly states that these certifications are not subject to judicial or administrative review.[150] But the Act gives Congress the power to prevent a proposed executive agreement from entering into force through expedited congressional review provisions after the certifications are provided.[151] Certifications must be renewed every five years, and recertifications trigger Congress's power to block renewal through expedited review processes.[152] Additionally, if requested by the Committees on the Judiciary or Foreign Affairs in the House or the Committees on the Judiciary or Foreign Relations in the Senate, the executive branch must furnish to the requesting committee a summary of the factors it considered when determining that a foreign government satisfies the CLOUD Act's requirements.[153]

[147] The CLOUD Act provides that the factors "to be met" when determining whether a foreign government affords the requisite protections for privacy and civil liberties include the following: whether the foreign government (1) has "adequate" laws related to cybercrime and electronic evidence as demonstrated by being a party to the Convention on Cybercrime, entered into force Jan. 7, 2004, 41 I.L.M. 282, 2296 U.N.T.S. 167 (known as the Budapest Convention) or through domestic law consistent chapters I and II of the Budapest Convention; (2) demonstrates "respect for rule of law and principles of nondiscrimination;" (3) "adheres to international human rights obligations and commitments or demonstrates respect for international universal human rights[;]" (4) "has clear legal mandates and procedures" governing its entities that are authorized to seek data, including procedures through which those authorities "collect, retain, use, and share data, and effective oversight of those activities;" (5) has "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data[;]" and (6) "demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet . . . ." *See* CLOUD Act § 105.

[148] For background on decryption, see CRS Report R44642, *Encryption: Frequently Asked Questions*, by Chris Jaikaran, at 2.

[149] *See* CLOUD Act § 105 (adding 18 U.S.C. § 1253).

[150] *Id.* ("A determination or certification made by the Attorney General . . . shall not be subject to judicial or administrative review.").

[151] The procedures for expedited review in Congress are discussed *infra* § Congressional Review of CLOUD Act Agreements.

[152] *See* CLOUD Act § 105 (adding 18 U.S.C. § 1253).

[153] The CLOUD Act requires that a proposed agreement and the Attorney General's certifications be transmitted to the Committees on the Judiciary and Foreign Affairs in the House of Representatives and the Committees on the Judiciary and Foreign Relations in the Senate. *See id.*

Limitations on Orders Issued Under CLOUD Act Agreements

The fourth certification required by the CLOUD Act mandates that any data sharing agreement concluded under the Act contain a set of requirements related to foreign governments' orders issued to service providers. These include, among things,[154] requirements that all orders

- identify a specific person, account, or other identifier that is the object of the order;[155]
- be premised on a "reasonable justification based on articulable and credible facts, particularity, and severity regarding the conduct under investigation";[156]
- 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;
- be issued for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution or a "serious "crime"—a term that the CLOUD Act states includes terrorism, but otherwise does not define;[157]
- comply with the domestic law of the issuing country;
- not be used to infringe freedom of speech; and
- satisfy additional requirements for real-time communications captured by wiretap.[158]

When a foreign government receives the requested data from the provider, it must promptly review the material and store any unviewed communications on a "secure system accessible only to those trained in applicable procedures . . . ."[159] The "applicable procedures" must, to the maximum extent possible, comply with the minimization procedures in Section 101 of the Foreign Intelligence Surveillance Act (FISA).[160] Foreign governments may not issue an order at the request of the United States or any third-party government, and they may not disclose the content of communications of a U.S. person to the U.S. government except in cases involving significant harm or threat of harm to the United States or U.S. persons.[161]

Mandatory Rights Granted to the United States

The CLOUD Act requires that data sharing agreements grant certain powers to the U.S. government. Specifically, the foreign government must grant reciprocal rights of data access to

[154] The description of requirements for CLOUD Act agreements in the body of this report is not exhaustive. A complete list of requirements is contained in Section 105 of the Act.

[155] *See* CLOUD Act § 105 (adding 18 U.S.C. § 1253).

[156] *See id.*

[157] *See id*.

[158] Wiretap orders must be for a fixed, limitation duration; may not last longer than is reasonably necessary to accomplish the purposes of the order; and can be issued only if the information could not be obtained with less intrusive methods. *See id*.

[159] *Id.*

[160] See 50 U.S.C. § 1801(h). For background on FISA and its minimization procedures, see CRS Report R44457, *Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, by Edward C. Liu, at 2-4, and Congressional Distribution Memorandum from Edward C. Liu, Legislative Attorney, Cong. Research Serv., Summary of Substantive Provisions of S. 2010, the FISA Amendments Reauthorization Act of 2017, H.R. 3989, the USA Liberty Act of 2017, and S. 139, the FISA Amendments Reauthorization Act of 2017, at 7-17 (available upon request from the author).

[161] *See* CLOUD Act § 105 (adding 18 U.S.C. § 1253).

the United States and allow the U.S. government to conduct periodic reviews of the foreign nation's compliance with the terms of the executive agreement.[162] CLOUD Act agreements also must reserve the United States' right to "render the agreement inapplicable" for any order for which the United States concludes the agreement "may not properly be invoked."[163]

Judicial or Governmental Review of Orders Under CLOUD Act Agreements

The process for judicial or other government oversight of foreign nations' requests for data under the CLOUD Act differs from earlier international data sharing regimes. In both the MLAT and letters rogatory processes, a federal court reviews and approves a foreign government's request for information before issuing a warrant or court order.[164] Such requests generally must satisfy U.S. legal standards and constitutional requirements, such as the Fourth Amendment probable cause standard.[165] Several federal appellate courts have stated that an otherwise valid MLAT or letters rogatory request may be rejected if compliance would result in a violation of the Constitution.[166] For MLAT requests, agencies in the executive branch conduct additional reviews for compliance with U.S. law before and after receiving judicial approval to execute a cross-border data request.[167]

Under CLOUD Act agreements, by contrast, foreign governments can submit orders directly on service providers.[168] While those orders are "subject to review or oversight by a court, judge, magistrate, or other independent authority" in the *foreign nation*, the CLOUD Act does not require review or approval by a U.S. court or federal agency.[169] And unlike MLATs and letters rogatory, the CLOUD Act contemplates that the judicial or other independent review in the foreign country could occur *after* a foreign government issued an order to a service provider.[170] The ultimate result is that foreign nations' orders issued under the CLOUD Act are not required to undergo individualized review by any branch of the U.S. government, and U.S. courts are not required to analyze whether the foreign government's request complies with U.S. constitutional standards. This change appears to be intended to accelerate the data sharing process, especially in cases involving emergency or other time-sensitive requests.[171] Rather than review each request individually, the United States' opportunity to scrutinize a foreign country's data demands primarily will occur during the periodic review of a foreign nation's compliance with its data

[162] *See id*.

[163] *Id.*

[164] *See* FUNK, *supra* note 16, at 10-11, 18-19.

[165] *See* Kendall & Funk, *supra* note 107, at 60 ("[Federal judges . . . serve as the gatekeepers for search warrants, wiretaps, and other methods of obtaining evidence, ensuring that the requested foreign evidence collection meets the same standards as those required in U.S. cases . . . for example, finding probable cause . . . ."); Woods, *supra* note 1, at 783 ("Under the current ECPA regime, foreign law enforcement officials must prove to a U.S. judge that they have probable cause (the Fourth Amendment standard) to obtain a warrant.").

[166] *See supra* note 122.

[167] *See* Swire & Hemmings, *supra* note 101, at 696-700.

[168] *See* CLOUD Act § 104.

[169] *Id.* § 105 (adding 18 U.S.C. § 1253).

[170] *See id.* (providing that judicial or independent review must take place "prior to, *or* in proceedings regarding, enforcement of the order . . . .") (emphasis added).

[171] *See*, *e.g.*, Downing Statement, *supra* note 1, at 9 (contending that legislative reform to the MLAT process is necessary to allow more expedient access to digital evidence); McGuinness Statement, *supra* note 3 (same).

sharing agreements and when evaluating whether a foreign nation's laws satisfy the CLOUD Act's eligibility requirements.[172]

What Nations Are Eligible for CLOUD Act Agreements?

The CLOUD Act does not specify by name what countries meet its requirements, and the Attorney General has not provided the requisite certifications for a proposed agreement as of the date of this report. Consequently, it is not clear which, if any, nations may be eligible for CLOUD Act agreements. However, in 2016, DOJ informed Congress that the United States sought legislation that would implement a potential bilateral data sharing agreement with the United Kingdom.[173] While the draft bilateral agreement has not been made public, DOJ proposed legislation that the department stated was necessary to implement the potential agreement.[174] The structure and many provisions of the CLOUD Act appear to have been derived—and in some cases taken verbatim—from DOJ's proposed legislation.[175] Some commentators believe that the U.S.-U.K. agreement will be the first agreement to be certified by the executive branch and submitted to Congress for review under the CLOUD Act's expedited congressional review procedures, as discussed below.[176]

Congressional Review of CLOUD Act Agreements

The CLOUD Act provides for a mandatory 180-day period of congressional review before a proposed data sharing agreement can enter into force.[177] The Act also defines a number of procedures authorizing congressional consideration of a joint resolution of disapproval of an executive agreement on an expedited process. The procedures include among other things, automatic discharge of the congressional committees to whom the joint resolution has been referred within 120 days;[178] waiver of certain points of order; limitations on and structuring of

---

[172] *Cf.* LIN & FIDLER, *supra* note 93, at 5 ("[O]rders do not undergo individual inspection by the U.S. government, making the vetting of countries for the executive agreement the single guaranteed point of scrutiny.").

[173] *See* Kadzik Letter, *supra* note 92 ("The legislative proposal is necessary to implement potential bilateral agreement between the United Kingdom and the United States that would permit U.S. companies to provide data In response to U.K. orders targeting non-U.S. persons located outside the United States, while affording the United States reciprocal rights . . . .").

[174] *See* Legislation to Permit the Secure and Privacy-Protective Exchange for Electronic Data for the Purposes of Combating Serious Crime Including Terrorism [hereinafter 2016 Proposed U.S.-U.K. Legislation] *in* Kadzik Letter, *supra* note 92.

[175] *Compare*, *e.g.*, 2016 Proposed U.S.-U.K. Legislation, *supra* note 174, § 2(1) ("Timely access to electronic data held by communications-service providers is an essential component of government efforts to protect public safety and combat serious crime, including terrorism . . . ."), *with* CLOUD Act § 102(1) (identical language). DOJ proposed amending ECPA to add an extraterritoriality provision in response to *Microsoft* in a draft bill circulated in 2017. *See supra* note 68. That 2017 proposal incorporated the provisions authorizing data sharing executive agreements from DOJ's 2016 proposal. *See id.*

[176] *See*, *e.g.*, Thomas P. Bossert & Paddy McGuinness, Opinion, *Don't Let Criminals Hide Their Data Overseas*, N.Y. TIMES (Feb. 15, 2018), https://www.nytimes.com/2018/02/14/opinion/data-overseas-legislation.html ("The bill would authorize the attorney general to enter into such agreements, but only with allies that respect privacy and protect civil liberties, and that have records of promoting and defending due process. The first one would be with Britain, which already has the authority to enter into such a pact."); Jennifer Daskal, *New Bill Would Moot Microsoft Ireland Case—And Much More!*, JUST SECURITY (Feb. 6, 2018), https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more/ ("[T]he legislation would authorize the executive to finalize a draft executive agreement with the UK that was negotiated during the Obama presidency . . . .").

[177] CLOUD Act § 105 (adding 18 U.S.C. § 1253).

[178] A joint resolution of disapproval is automatically referred to the House Committees on the Judiciary and Foreign Affairs and the Senate Committees on the Judiciary and Foreign Relations. *Id.* Whereas Congress's 180-day period to (continued...)

debate; and expedited treatment of a joint resolution received from the other chamber of Congress.[179]

If Congress enacts a joint resolution of disapproval during the 180-day review window, the CLOUD Act states that the proposed agreement may not enter into force.[180] Such a joint resolution of disapproval would require passage by both chambers of Congress and the President's signature or a veto override.[181] Because the CLOUD Act provides that proposed data sharing agreements will be submitted to Congress after already receiving the approval of two Cabinet-level executive officials—the Attorney General and Secretary of State—some commentators contend that a President would be unlikely to sign a joint resolution of disapproval, making a veto-proof majority necessary to block a proposed CLOUD Act agreement.[182]

Commentary on the CLOUD Act

The CLOUD Act has garnered both praise and criticism from observers.[183] Some argue that the Act provides a practical remedy for problems related to the globalization of evidence and the increased demand for data stored overseas in criminal cases.[184] Supporters assert that the need for data stored abroad, which often is held by U.S. internet companies, has overburdened the legal architecture established in the MLAT and letters rogatory systems, rendering those systems "outdated and inefficient."[185] Supporters also argue that the CLOUD Act provides adequate protection for privacy, civil liberties, and human rights.[186] They contend that, absent the change in law, frustrated foreign governments that are unable to obtain data held by U.S. companies will exert extraterritorial application of their own laws or enact data localization laws[187] that some

(...continued)

vote on a joint resolution of disapproval commences on the date on which the Attorney General provides a copy of the proposed agreement to Congress, the 120-day clock for committee consideration begins to run on the date of referral of a joint resolution. *Id.*

[179] *See id*.

[180] *See id*.

[181] *See Legislation, Laws, and Acts*, U.S. SENATE (last visited Apr. 5, 2018), https://tinyurl.com/yaun8wry ("Like a bill, a joint resolution requires the approval of both Chambers in identical form and the president's signature to become law. There is no real difference between a joint resolution and a bill.").

[182] *See*, *e.g.*, Neema Singh Gullani & Naureen Shah, *The CLOUD Act Doesn't Help Privacy and Human Rights: It Hurts Them*, LAWFARE (Mar. 16, 2018), https://lawfareblog.com/cloud-act-doesnt-help-privacy-and-human-rights-it-hurts-them; Robyn Greene, *Four Common Sense Fixes to the CLOUD Act that its Sponsors Should Support*, JUST SECURITY (Mar. 13, 2018), https://www.justsecurity.org/53728/common-sense-fixes-cloud-act-sponsors-support/.

[183] *See infra* notes 184-190.

[184] *See*, *e.g.*, Bossert & McGuinness, *supra* note 176; Lisa Monaco & John P. Carlin, Opinion, *A "Global Game of Whack-a-Mole": Overseas Data Rules are Stuck in the 19th Century*, WASH. POST (Mar. 5, 2018), https://tinyurl.com/ybghkrhn; Andrew Keane Woods, Peter Swire, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

[185] *See* LIN & FIDLER, *supra* note 93, at 4.

[186] *See*, *e.g.*, Jennifer Daskal, Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), https://www.lawfareblog.com/why-cloud-act-good-privacy-and-human-rights.

[187] Data localization laws require technology companies to store data on servers within nations' respective borders, thereby potentially obviating the need for cross-border data requests. *See*, *e.g.*, Bret Cohen, Britanie Hall, Charlie Wood, *Data Localization Laws and Their Impact on Privacy, Data Security and the Global Economy*, ANTITRUST, Fall 2017, at 107 ("Russia, China, Indonesia, and others have enacted explicit 'forced' localization requirements applicable to broad swaths of industry that require data to be stored on servers within their respective borders . . . ."); William Alan Reinsch, *A Data-Localization Free-for-all?*, CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (Mar. 9, 2018), https://www.csis.org/blogs/future-digital-trade-policy-and-role-us-and-uk/data-localization-free-all#_ednref1 ("The (continued...)

believe impede the effective functioning of an open internet.[188] Several major U.S. technology companies—including Apple, Facebook, Google, Microsoft, and Oath—support the legislation, calling it an effective legislative solution that reduces conflicts of laws.[189]

Critics of the CLOUD Act argue that it poses a threat to civil liberties and human rights by lowering the standards previously necessary to obtain evidence in cross-border criminal investigations and prosecutions.[190] They contend that the CLOUD Act's standard for individualized suspicion—"reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"—is vague and may not rise to the level of probable cause necessary to obtain a judicial warrant under U.S. law.[191] Some argue that the executive branch's decision to certify a country as satisfying the CLOUD Act's standards should be subject to judicial or other review.[192] Others contend that the concept that foreign nations' data requests do not need individualized review if the nations' domestic laws meet the Act's eligibility criteria is flawed because foreign governments' real-world operations may not comport with their domestic laws and may change over time.[193] Several critics of the CLOUD Act argue that it should require a foreign court or independent authority to approve a foreign government's order before the order is issued on a U.S. provider.[194] Others contend, among other things, that the law should increase the requirements for foreign governments to obtain access to real-time communications to the same standards that apply to the United States' interception of live communications in the Wiretap Act.[195]

(...continued)

degree of data localization measures worldwide has increased dramatically, most drastically since 2010."). For a survey of global data localization measures, see Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 682-712 (2015).

[188] *See, e.g.*, LIN & FIDLER, *supra* note 93, at 4; Jennifer Daskal, Peter Swire, *Privacy and Civil Liberties Under the CLOUD Act: A Response*, LAWFARE (Mar. 21, 2018), https://www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response.

[189] *See* Letter from Apple et al. to Representative Doug Collins et al. (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-House-CLOUD-Act-020618.pdf.

[190] *See, e.g.*, Sharon Bradford Franklin, Director of Surveillance & Cybersecurity Policy, New America, Open Technology Institute, *OTI Opposes the CLOUD Act*, OPEN TECHNOLOGY INSTITUTE (Feb. 6, 2018), https://www.newamerica.org/oti/press-releases/oti-opposes-cloud-act/; Gullani & Shah, *supra* note 182; Robyn Greene, *Somewhat Improved, the CLOUD Act Still Poses a Threat to Privacy and Human Rights*, JUST SECURITY (Mar. 23, 2018), https://www.justsecurity.org/54242/improved-cloud-act-poses-threat-privacy-human-rights/.

[191] *See* Gullani & Shah, *supra* note 182. *See also* Franklin *supra* note 190; Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Snooping on Cross-Border Data*, ELECTRONIC FRONTIER FOUNDATION (Feb. 8, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data; *CLOUD Act Would Erode Trust in Privacy of Cloud Storage*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Feb. 6, 2018), https://cdt.org/press/cloud-act-would-erode-trust-in-privacy-of-cloud-storage/.

[192] *See, e.g.*, Franklin *supra* note 190.

[193] *See* Gullani & Shah, *supra* note 182 ("The very premise of the current CLOUD Act—the idea that countries can effectively be safe-listed as human-rights compliant, such that their individual data requests need no further human rights vetting—is wrong.").

[194] *See, e.g.*, Daniel Sepulveda, Opinion, *Bill on Cross-Border Data Access Needs to Change, Despite Laudable Goal*, THE HILL (Mar. 16, 2018), http://thehill.com/opinion/technology/378785-bill-on-cross-border-data-access-needs-to-change-despite-laudable-goal; Greene, *supra* note 190; Franklin *supra* note 190.

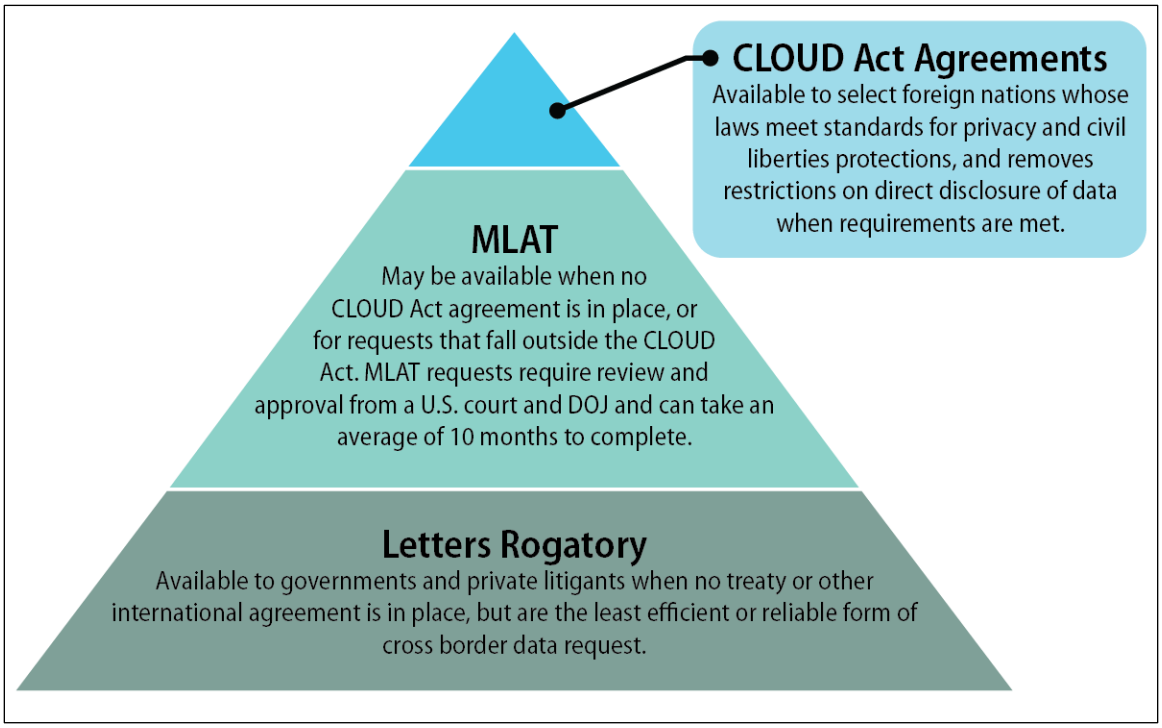
[195] *See* Fischer, *supra* note 191; Greene, *supra* note 190; Gullani & Shah, *supra* note 182.

How Will CLOUD Act Agreements Interact with Existing Data Sharing Processes?

Executive agreements authorized by the CLOUD Act would supplement, not replace, existing avenues of international data sharing.[196] Accordingly, requests for assistance would still be available through MLATs (when in effect) and letters rogatory.

When analyzed in light of existing data sharing processes, the CLOUD Act has the potential to result in a three-tiered system for cross-border data sharing in criminal matters. Those nations that are approved for CLOUD Act agreements could request data directly from U.S. service providers in cases involving "serious crimes"—provided they do not target U.S. persons or persons located in the United States and meet the CLOUD Act's other requirements.[197] For nations that have an MLAT but no CLOUD Act agreement, or for data requests that fall outside the scope of the CLOUD Act, foreign governments can use the MLAT process.[198] Finally, private litigants and nations that do not have a CLOUD Act agreement or an MLAT may request that their courts issue letters rogatory to the courts of the United States.[199]

Figure 1. Three Tiers of Cross-Border Data Sharing



Source: *Supra* §§ Letters Rogatory; Mutual Legal Assistance Treaties (MLATs); Executive Agreements Authorized by the CLOUD Act.

[196] *See* CLOUD Act § 106.

[197] *See supra* § Requirements for CLOUD Act Agreements.

[198] *See supra* § Mutual Legal Assistance Treaties (MLATs).

[199] *See supra* § Letters Rogatory.

Conclusion

While the CLOUD Act is likely to more clearly define the scope of U.S. officials' right to seek certain data stored overseas in the custody of U.S. providers, its broader impact on the international data sharing regime is less certain. As the internet continues to expand and become more globalized, law enforcement officials worldwide can be expected to continue to seek access to data stored on servers outside their territorial jurisdictions.[200] Although the major technology companies responsible for maintaining a large share of the world's data are located in the United States,[201] the United States accounts for less than 10% of the estimated 3 billion internet users worldwide.[202] These demographics potentially could lead many nations to pursue CLOUD Act agreements, which would provide faster access to data held by U.S. providers. Whether the United States ultimately enters such agreements will depend on the willingness of the executive branch to certify foreign nations' eligibility and Congress's desire to block a proposed agreement through a joint resolution of disapproval enacted into law.

The impact of the CLOUD Act on privacy, human rights, and civil liberties interests similarly is difficult to predict.[203] The Act has the potential to create a three-tiered system of international data sharing, with the United States' most trusted foreign partners able to obtain data directly from U.S. companies without individualized review by the U.S. government.[204] Because this system of direct access differs from existing international data sharing regimes, the manner in which data requests are administered, the type of data that is collected, and the degree of potential for abuse of the system, if any, may become more apparent over time.

Author Contact Information

Stephen P. Mulligan
Legislative Attorney
smulligan@crs.loc.gov, 7-8983

[200] *See, e.g.*, Woods, *supra* note 1, at 741-42 (discussing shifts in expansion of internet usage across the globe); *Chapter One Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance*, 131 HARV. L. REV. 1722 (2018) ("[T]echnology companies have become major actors in the world of law enforcement and national security.").

[201] *See supra* note 93.

[202] Woods, *supra* note 1, at 741.

[203] *Cf.* Tom Kulik, *Stormy Weather: How the Cloud Act May Rain on the Privacy of Data*, ABOVE THE LAW (Apr. 13, 2018), https://tinyurl.com/y82ze95b ("[T]he Cloud Act has definitely created some unpredictable weather. . . .").

[204] *Cf.* Moskowitz, *supra* note 103, at 2 (discussing the potential formation of a so-called "Trusted Nations Club" in the context of international data sharing); Swire and Hemmings, *supra* note 101, at 690 (analogizing a cross-border data sharing regime to the Visa Waiver Program in which citizens of a group of developed nations can bypass certain requirements for travel to the United States).