Issue Brief February 2020

Overcoming Constitutional Objections to the CLOUD Act

Peter Swire & Justin Hemmings

Introduction

In 2018, the U.S. passed the Clarifying Lawful Overseas Use of Data Act (the "CLOUD Act" or "Act") in response to two related but distinct issues. The first part of the Act clarifies rules governing *U.S. law enforcement access* to data in the hands of U.S. providers, and in doing so mooted the pending Supreme Court case *United States v. Microsoft* (the "Microsoft Ireland" case). Microsoft argued that a U.S. warrant had no legal force to compel the production of emails stored on a server in Ireland. To resolve that question of law, the first part of the CLOUD Act provides that compelled disclosure orders issued by the U.S. will apply "regardless of whether such communication, record, or other information is located within or outside of the United States."[1]

The second part of the CLOUD Act responds to *foreign governments' access* to data in the hands of U.S. providers. Under the Stored Communications Act (SCA),[2] which is part of the Electronic Communications Privacy Act (ECPA),[3] service providers are generally prohibited from responding to a foreign government request for the content of communications except upon receipt of a court order signed by a U.S. judge. This prohibition applies even when the foreign government seeks to access data regarding its own nationals in the investigation of a local crime. With the prevalence of cloud computing, evidence for ordinary criminal investigations increasingly is held on servers in different countries. A 2018 report by the European Commission found that "more than half of all investigations involve a cross-border request to access [electronic] evidence."[4] This shift towards the "globalization of criminal evidence" creates major difficulties for law enforcement.[5] The traditional cross-border mutual legal assistance (MLA) mechanisms, such as mutual legal assistance treaties (MLATs) and letters

[1] 18 U.S.C. § 2713. *See* Jennifer Daskal, *Access to Data Across Borders: The Critical Role for Congress to Play Now*, AM. CONST. SOC'Y (Oct. 24, 2017).
[2] 18 U.S.C. §§ 2701–2713.
[3] *Id.* §§ 2510–2523.
[4] COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT, EUROPEAN COMM'N (Apr. 17, 2018).
[5] Daskal, Swire & Christakis, *The Globalization of Criminal Evidence*, Int'l Ass'n of Privacy Prof'ls (Oct. 18, 2018).

rogatory, are slow and cumbersome. For example, the average length of time for the U.S. to respond to an MLAT request is reportedly at least 10 months.[6] To supplement the current MLA procedures, the second part of the CLOUD Act creates a new system of "executive agreements" designed to speed the access of foreign law enforcement to data where the Act's privacy and human rights safeguards are met.[7]

The CLOUD Act thus responds to obstacles that both U.S. and foreign law enforcement face with the shift to cloud computing, with the evidence so often held abroad. There are sharp disputes about whether the Act overall is likely to increase or decrease privacy protections. Given these privacy concerns, privacy advocates might raise constitutional challenges to the CLOUD Act.

On October 3, 2019, the U.S. and U.K. signed the first CLOUD Act executive agreement, providing an opportunity to raise these challenges.[8] This agreement is likely to come under particularly close scrutiny as it could serve as a model for subsequent agreements and will test the Act's congressional review process. Civil society groups have written to the relevant House and Senate committees to raise objections to the U.S.-U.K. agreement, including that the agreement "permits the U.K. to share information with the U.S. government about Americans, collected under standards that fall short of the Fourth Amendment."[9] These and other interested parties may similarly challenge the agreement in court, if it survives congressional review.

Part I of this Issue Brief provides a brief history of the CLOUD Act and the context in which it was passed. Part II examines the privacy debates around the CLOUD Act as a policy matter, and whether it is a net positive or negative for privacy rights. Part III provides what we believe is the first analysis of potential facial and as-applied constitutional challenges to the CLOUD Act under the Fourth Amendment. Our discussion highlights factors such as state action, covered persons, whether foreign governments may act as an agent of the United States, and possible issues with incidental collection of protected persons' data. We conclude that in the absence of a strong fact pattern for plaintiffs, it would appear difficult to overturn the CLOUD Act on Fourth Amendment grounds. Finally, Part IV discusses possible next steps for implementation of the CLOUD Act.

---

[6] PETER SWIRE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD 227 (Dec. 12, 2013).

[7] The executive agreement approach was proposed in Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, 71 N.Y.U. ANNUAL SURVEY OF AM. L. 687, 725–38 (2016). *See Cross-Border Requests for Data Project*, GA. TECH INST. FOR INFO. SEC. & PRIVACY (last visited Jan. 16, 2020).

[8] *U.S. and UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, U.S. DEP'T OF JUSTICE (Oct. 3, 2019).

[9] Letter from Access Now et al., to Sen. Lindsey Graham, Chairman, U.S. Senate Committee on the Judiciary et al. (Oct. 29, 2019).

I. The CLOUD Act

The SCA, passed in 1986 and written before there was any such thing as a global Internet, has been widely interpreted to prohibit U.S. service providers from disclosing communications content directly to foreign governments in response to otherwise valid legal orders. Instead, foreign governments must submit a diplomatic request through an MLAT. The MLAT process is a lengthy one, taking ten months on average to complete, that requires foreign governments to demonstrate probable cause sufficient to support a warrant under the U.S. Constitution's Fourth Amendment.[10]

When MLATs were first introduced, law enforcement tended to use this process in exceptional circumstances, such as international money laundering and drug trafficking investigations. Since then, however, the globalization of criminal data has created more demand for and stress on this system. More and more frequently, the evidence law enforcement is seeking is stored in the cloud, and often on servers residing in a foreign country's jurisdiction.[11]

Governments and service providers had both long-sought ways to reform the MLAT system and more efficiently address the increasing volume of requests. Foreign governments had been increasingly frustrated with the timeframe to respond to MLAT requests, and with having to comply with U.S. law in situations where the only nexus to the U.S. is that the data is held by a U.S. service provider. At the same time, service providers increasingly found themselves caught between two irreconcilable legal obligations—being required to produce content under the law of a foreign government on the one hand and prohibited by the U.S. from producing it under the SCA on the other. Companies found themselves subject to increasing pressure from foreign governments to comply with requests regardless of U.S. law, including detaining employees that fail to comply with orders to produce evidence and an increasing number of national data localization requirements.[12]

The CLOUD Act was an attempt to mediate these concerns and provide a path forward for cross-border data requests. The Act affected two major changes to the existing MLA landscape. First, it amended the SCA to state explicitly that the determining factor for whether U.S. service providers must comply with a compelled disclosure order is whether or not the U.S. service provider has "possession, custody, or control" of the specified evidence.[13] Second, it created the

---

[10] Swire & Hemmings, *supra* note 7, at 697–700.

[11] Peter Swire & Jennifer Daskal, *What the CLOUD Act Means for Privacy Pros*, INT'L ASS'N OF PRIVACY PROF'LS (Mar. 26, 2018).

[12] Brad Haynes, *Facebook Executive Jailed in Brazil as Court Seeks WhatsApp Data*, REUTERS (Mar. 1, 2016); Kalika Likhi, *India's Data Localization Efforts Could Do More Harm Than Good*, ATLANTIC COUNCIL (Feb. 1, 2019); Matthew Newton & Julia Summers, *Russian Data Localization Laws: Enriching "Security" & the Economy*, HENRY M. JACKSON SCH. OF INT'L STUDIES (Feb. 28, 2018); Mai Nguyen, *Exclusive: Vietnam Cyber Law Set for Tough Enforcement Despite Google, Facebook Pleas*, REUTERS (Oct. 10, 2018).

[13] The Act amended 18 U.S.C. § 2713 to read

executive agreement system whereby "qualified foreign governments" can demand the production of electronic communications directly from U.S. service providers. These "qualified foreign governments" could, in return for meeting certain privacy and civil liberty requirements, enter into a CLOUD Act executive agreement that permits them to issue domestic legal process directly to U.S.-based service providers thereby making it easier to access electronic communications.

For each executive agreement, the U.S. Attorney General, in consultation with the U.S. Secretary of State, must certify that the foreign government meets certain baseline substantive and procedural requirements. These requirements, which are statutorily mandated, require respect for applicable international human rights obligations, such as freedom from arbitrary arrest and detention, as well as clear legal procedures governing data requests.[14]

Each executive agreement must also contain protections designed to assure compliance with the Fourth Amendment. To that end, the CLOUD Act prohibits foreign governments from intentionally targeting for surveillance the communications of any U.S. person or person located in the United States.[15] Additionally, the CLOUD Act prohibits a foreign government from issuing an order at the request of or on behalf of the U.S. government.[16] The foreign government may only share with U.S. authorities the contents of a U.S. person communication if it relates to

---

> 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.

In other words, a company that receives valid process served pursuant to the SCA has a U.S. legal obligation to disclose relevant evidence in its "possession, custody, or control," regardless of where the company keeps its servers.

[14] The requirements to be a "qualified foreign government" can be found in 18 U.S.C. § 2523(b)(1)(B). These requirements include: Demonstrating respect for the rule of law and principles of nondiscrimination; Adhering to applicable international human rights obligations and demonstrating respect for international human rights such as protection from arbitrary and unlawful interference with privacy, fair trial rights, prohibitions on arbitrary arrest and detention, and prohibitions against torture and cruel, inhuman, or degrading punishment; Having clear legal mandates and procedures governing its entities that are authorized to seek data under an executive agreement, including effective oversight; Having sufficient mechanisms to provide accountability and transparency for the government's collection and use of electronic data; Demonstrating a commitment to promote and protect the global free flow of information and an open and interconnected Internet; and Adopting "appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons" that would be subject to the executive agreement.

[15] 18 U.S.C. § 2523(b)(4)(A). Similarly, the law prohibits intentionally targeting a non-U.S. person located outside the U.S. for the purpose of obtaining information concerning a U.S.-person or a person located in the U.S. *Id.* § 2523(b)(4)(B).

[16] *Id.* § 2523(b)(4)(C).

"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."[17] Even then, the communication is subject to minimization requirements.

These requirements set a floor, not a ceiling, for what is included in an executive agreement. The parties may negotiate additional requirements beyond those listed in the CLOUD Act itself. Additional terms could be included based on the specific concerns presented by a foreign government's legal system,[18] and a number of such safeguards were included in the U.S.-U.K. Agreement.[19] This flexibility may allow countries outside of the closest American allies, such as India, to negotiate their way into an executive agreement by agreeing to additional terms outside of those that are statutorily required.[20]

After the executive agreement has been negotiated, the U.S. Attorney General, in consultation with the U.S. Secretary of State, must certify in writing to Congress that the executive agreement meets the Act's requirements, including an explanation of each consideration underlying the certification.[21] After they do so, the agreement enters into force unless, within 180 days of being notified, the House or Senate introduces a joint resolution of disapproval. If after 120 days the relevant committee has not acted on the resolution, the resolution is discharged and placed on the appropriate calendar for consideration.[22] The resolution then must be passed by Congress and signed by the President (or the President's veto must be over-ridden) to prevent the agreement from entering into force. Agreements also must be re-certified every five years to Congress via a report from the Attorney General, in consultation with the Secretary of State, describing (1) the reasons for the renewal; (2) 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 (3) how the agreement has been implemented and what problems or controversies, if any, have arisen as a result of the agreement or its implementation.[23]

---

[17] *Id.* § 2523(b)(4)(H). These limitations track, although are not identical to, key protections in the Wiretap Act. *See id.* § 2518(1).

[18] Peter Swire & Justin Hemmings, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the CLOUD Act*, LAWFARE (Sep. 13, 2018); Jennifer Daskal & Peter Swire, *A Possible EU-US Agreement on Law Enforcement Access to Data?*, LAWFARE (May 21, 2018); Peter Swire & Deven Desai, *A "Qualified SPOC" Approach for India and Mutual Legal Assistance*, LAWFARE (Mar. 2, 2017).

[19] Jennifer Daskal & Peter Swire, *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019). We discuss details about these safeguards in the Conclusion, below.

[20] *See* Peter Swire et al., *India-US Data Sharing for Law Enforcement: Blueprint for Reforms*, OBSERVER RESEARCH FOUND. (Jan. 17, 2019).

[21] 18 U.S.C. §§ 2523(b), (g).

[22] *Id.* § 2523(5).

[23] *Id.* § 2523(e).

II. Fourth Amendment Implications

Prior to its passage, a group of 24 privacy, civil liberties, and human rights organizations signed a joint, open letter urging Congress to oppose the CLOUD Act.[24] The letter argued that the CLOUD Act would undermine rights for both U.S. and non-U.S. persons and would, among other concerns, allow foreign governments to obtain information that could pertain to individuals in the U.S. without meeting constitutional standards.[25] Their concern arises from the differing standards applied to requests for assistance pursuant to an MLAT and the CLOUD Act. Under an MLAT, a foreign government request for assistance must be approved by a U.S. judge, under the same probable cause standards that apply for a domestic case. By contrast, under the CLOUD Act, a qualifying foreign government could issue orders to produce evidence pursuant to its own domestic laws. Although the CLOUD Act sought to assure Fourth Amendment compliance by providing that 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,"[26] the letter expressed concerns over "incidental collection" of U.S. person data or those located in the U.S.[27]

These criticisms of the CLOUD Act are misplaced,[28] but the groups' concerns about the Fourth Amendment deserve a thoughtful analysis. In this section we turn to possible Fourth Amendment challenges. Such challenges could come from civil society groups who claim that an executive agreement is facially unconstitutional, or in the context of an individual prosecution raising an as-applied challenge. Challenges may also come from electronic service providers that receive demands for electronic evidence, as occurred in the *Microsoft Ireland* case.

A. The Scope of Fourth Amendment Protections

The basic requirements of the Fourth Amendment are that all searches must be reasonable[29] and that warrants can be issued only by independent judges upon probable cause of a crime. The

---

[24] Coalition Letter on CLOUD Act, ACLU (Mar. 12, 2018).

[25] *Id.* The CLOUD Act and other federal laws define a "U.S. person" as a U.S. citizen or legal permanent resident. *See, e.g.*, 18 U.S.C. § 2523(a)(2) (under U.S. criminal law "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."); *see also* 50 U.S.C. § 1801(i) (similar definition as applied to foreign intelligence activities).

[26] 18 U.S.C. § 2523(b)(4)(A).

[27] "Incidental collection" about a U.S. person can occur, for instance, if the target of surveillance is a foreign person, who then calls or emails the U.S. person.

[28] Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018).

[29] Reasonableness analysis "permeate[s]" Fourth Amendment search and seizure jurisprudence. "[It] is always the touchstone of Fourth Amendment analysis." County of Los Angeles v. Mendez, 137 S. Ct. 1539, 1546 (2017) (quoting *Birchfield v. North Dakota*, 136 S. Ct. 2160, 2186 (2016)). But the definitional boundaries of a reasonable search are murky because what is considered reasonable has evolved over time. Historically, the Court categorized warrantless searches as *per se* unreasonable "subject only to a

U.S. also follows the "exclusionary rule," so that illegally obtained evidence, or its fruits, generally cannot be used in court. For our CLOUD Act discussion, we highlight two aspects of Fourth Amendment doctrine: state action and a search or seizure against a defined class of covered persons.

1. State Action

Under the state action doctrine, the Fourth Amendment only binds U.S. federal, state, and local government, including private agents acting on its behalf.[30] For instance, the Federal Bureau of Investigation or a state police officer is bound by the requirements of the Fourth Amendment. By contrast, the Fourth Amendment does not apply to a search by a private actor. For instance, a private individual may search a person's house while performing a burglary. That search is assuredly criminal, but the Fourth Amendment does not apply. Similarly, a search by a foreign government generally does not receive Fourth Amendment protections because there is no state action.

That said, if a foreign government or private party were acting under the direction of a U.S. governmental unit – acting as its "agent," – those actions would be subject to the Fourth Amendment.[31] For instance, if U.S. law enforcement instigates, helps plan or execute, or offers an incentive for a search, that may be sufficient to satisfy the state action requirement.[32] In the context of the CLOUD Act, if a foreign government is acting as an agent of the U.S. government when compelling production of data pursuant to a CLOUD Act executive agreement, a Fourth Amendment claim may be possible.

2. Search Against a Defined Class of Covered Persons

The U.S. constitution applies differently based on the nationality and geographic location of the person being searched.[33] The Fourth Amendment only protects persons that are deemed entitled

---

few . . . exceptions," but has altered its approach and now interprets "the text of the Fourth Amendment as simply requiring reasonableness" regardless of whether a warrant was granted. Cynthia Lee, *Reasonableness with Teeth: The Future of Fourth Amendment Reasonable Analysis*, 81 Miss. L.J. 1133, 1134–36 (2012). Today, the reasonableness of a search requires courts to "weigh[] the nature and quality of the intrusion on the individual's Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion." Mendez, 137 S. Ct. at 1546 (quoting *Tennessee v. Garner*, 471 U.S. 1, 8 (1985)).

[30] The "U.S. government" includes all U.S. federal, state, local, or other governmental units subject to the U.S. Constitution.

[31] Skinner v. Ry. Labor Exec. Ass'n, 489 U.S. 602, 614 (1989).

[32] Lugar v. Edmondson Oil Co., 457 U.S. 922, 937 (1982); United States v. Jacobsen, 466 U.S. 109,113 (1984); People v. McKinnon, 7 Cal.3d 899, 912 (1972); People v. Bennett, 17 Cal.4th 373, 384, fn.3 (1998).

[33] One of the authors, Swire, has written separately about when this sort of "discrimination" based on nationality is permitted under international human rights law. *See* Peter Swire, Deven Desai & Jesse Woo, *The Important, Justifiable, and Constrained Role of Nationality in Foreign Intelligence Surveillance*, HOOVER INST. (Jan. 2019). *See also* Hernandez v. Mesa, 137 S. Ct. 2003, 2006 (2017) ("petitions had failed to state a claim for a violation of the Fourth Amendment because Hernandez was a "Mexican citizen who had no

to U.S. constitutional protections, the so-called "class of covered persons." Generally speaking, those persons who receive constitutional protection are U.S. persons, whatever their location, as well as non-U.S. persons within the United States.

The leading case on this point is *United States v. Verdugo-Urquidez*.[34] *Verdugo* dealt with a search of a non-U.S. person that took place outside the U.S. while the target was in U.S. custody. The case's reasoning relies on distinguishing when the Fourth Amendment does and does not apply to non-U.S. persons. Under *Verdugo*, Fourth Amendment protections apply to a non-U.S. person when that person is physically within the U.S. The protections do not, however, apply to a non-U.S. person outside of the U.S.

B. When Foreign Government Searches May Trigger Fourth Amendment Challenges

Generally, actions of a *foreign government* do not trigger Fourth Amendment U.S. constitutional protections because there is either (1) no U.S. government state action or (2) the search is not against a class of covered persons. For instance, the French government might conduct searches in France of French citizens, but the U.S. constitution would not generally apply to those searches.

With that said, searches conducted by a foreign government can be subject to the Fourth Amendment in some limited circumstances. We analyze below factual situations where litigants may advance a Fourth Amendment claim: (1) where the foreign government acts as an agent of the U.S. government and fails to comply with the Fourth Amendment; (2) where the foreign government routinely violates the CLOUD Act's ban on searches of persons within the territory of the U.S.; and (3) where the foreign government uses an executive agreement to incidentally collect substantial information about U.S. persons.

1. Agent of the U.S. Government

State action may exist to trigger U.S. constitutional protections where the U.S. government instigates, helps plan or execute, or offers an incentive for a search. The CLOUD Act specifically forbids a qualifying foreign government from acting on behalf of or at the direction of the U.S. government.[35] The U.S.-U.K. executive agreement contains a similar prohibition. Article 5(4) of the U.S.-U.K. executive agreement implements that statutory requirement: "The Issuing Party may not issue an Order subject to this Agreement at the request of or to obtain information to

'significant voluntary connection' to the United states" and "was on Mexican soil at the time he was shot.").

[34] United States v. Verdugo-Urquidez, 494 U.S. 259, 271–72 (1990).

[35] 18 U.S.C. § 2523(b)(4)(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.").

provide to the Receiving Party or a third-party government."[36] In light of these prohibitions, a facial challenge to the CLOUD Act would likely fail.

In the absence of a facial challenge, the facts might support a Fourth Amendment claim as applied to a specific case. Such an as-applied challenge would most likely arise in defense of an individual prosecuted by the U.S. government. The hypothetical defendant would need to establish a strong enough role by the FBI or other U.S. government actor to argue that the foreign government was acting under the direction and control of the U.S. government. The defendant would then argue that the search was constitutionally "unreasonable" and invoke the exclusionary rule – the U.S. doctrine that says that fruits of an unconstitutional search may not be used in court – to exclude the evidence from the case.[37] With strong enough facts, a defendant could establish agency and win an as-applied challenge. In that instance, the government's action would be violating both the Fourth Amendment and the clear terms of the statute.

2. Foreign Search of a Non-U.S. Person in U.S. Territory

Fourth Amendment protections apply to searches by the U.S. government against non-U.S. persons within U.S. territory. A litigant might argue that the executive agreement, or actions pursuant to it, constitute state action for Fourth Amendment purposes when the search affects a non-U.S. person who is within U.S. territory.

This theory of state action appears quite weak on a facial challenge. First, the Fourth Amendment restricts what actions the U.S. government can take. It does not, however, create an affirmative obligation on the U.S. government to protect against actions taken by foreign governments. Second, the text of the CLOUD Act prohibits searches that would constitute state action. Specifically, the law prohibits any foreign government requests targeting U.S. persons or persons within U.S. territory. Third, the CLOUD Act changed the statutory protections created by the SCA. These Amendments do not appear to create any constitutional difficulty under the Fourth Amendment.

Although a facial challenge would appear to fail, there may be factual settings where foreign searches might trigger Fourth Amendment protections for non-U.S. persons in the U.S. Perhaps the strongest scenario is if the U.S. government knows that an executive agreement is routinely used to target non-U.S. persons within the U.S. In this scenario, there would be a stronger factual basis for a finding of U.S. state action – the U.S. may be complicit in permitting the

---

[36] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, U.S.-UK, art. 5(4), Oct. 3, 2019.

[37] Note that even if the foreign government's search were found to be bound by the Fourth Amendment, the evidence of the search itself may still be admissible based on an exception to the exclusionary rule. While a foreign government acting as an agent of the United States may present novel questions concerning these exceptions, we do not attempt to resolve those questions here.

foreign government to use the executive agreement to evade Fourth Amendment protections. However, as noted earlier, the Fourth Amendment does not require the U.S. government to protect U.S. persons from individual or recurring actions of a foreign government. Therefore, the case for state action remains weak.

U.S. government action may be easier to establish if there is knowledge of routine violations prior to renewal of an executive agreement. The CLOUD Act requires renewal every five years.[38] At the time of renewal, the Attorney General, after consultation with the Secretary of State, must determine that the foreign country meets the requirements of the CLOUD Act, including that the foreign government does not target persons in the U.S. Suppose that the Attorney General, knowing about routine violations of these CLOUD Act targeting rules, nonetheless certifies compliance with the CLOUD Act. Under these facts, the certification may constitute U.S. government state action, and thus a court would have a stronger basis for applying Fourth Amendment protections for searches done after that certification.

State action might also be found if the Department of Justice (DOJ) prosecutes someone based on information that a foreign government collected under a CLOUD Act agreement. Because the U.S. Government is subject to the Fourth Amendment, a defendant prosecuted by the DOJ could argue that a federal prosecution itself is sufficient state action to satisfy the constitutional requirement. Even here, however, the DOJ could contend that prosecutors are generally permitted to receive evidence voluntarily provided by others without it constituting state action.

3. Incidental Foreign Collection of U.S. Person Information

The ACLU coalition letter highlighted the concern that the CLOUD Act would "permit foreign governments to share incidentally collected data about Americans with U.S. governmental entities, even when obtained under standards lower than what the Constitution requires."[39] Such "incidental" collection might occur when a U.S. person communicates with a non-U.S. person target. A facial challenge under these circumstances appears quite weak. Even as-applied challenges will likely fail, unless there are egregious facts that violate the CLOUD Act's statutory requirements.

A facial challenge would need to overcome at least two significant obstacles – the CLOUD Act's targeting and minimization requirements, and a lack of state action. First, the CLOUD Act prescribes targeting requirements for executive agreements:

> 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.[40]

---

[38] 18 U.S.C. § 2523(e)

[39] Coalition Letter on CLOUD Act, *supra* note 26.

[40] 18 U.S.C. § 2523(b)(4)(A).

These CLOUD Act requirements prohibit targeting individuals subject to U.S. constitutional protections, namely, U.S. persons or a person located in the U.S.

Additionally, executive agreements must also include minimization procedures. A foreign government

> shall, using procedures that, **to the maximum extent possible**, meet the definition of minimization procedures[41] in [FISA], 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. (emphasis added)[42]

The statute's "significant harm" exception encompasses, among other things, terrorism, significant violent crime, child exploitation, transnational organized crime, and significant financial fraud.[43] In light of these statutory limits on targeting, storing, and disseminating

---

[41] Under FISA, "minimization procedures" are defined as

> (1) specific procedures … that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States person consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> (2) procedures that require that nonpublicly available information, which is not foreign intelligence information … shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
> (4) notwithstanding paragraphs (1), (2), and (3) … procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order … is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person. 50 U.S.C. § 1801(h).

[42] 18 U.S.C. § 2523(b)(4)(G).

[43] *Id.* § 2523(b)(4)(H). If the scope of this exception for terrorism and other crimes were to be litigated, the Department of Justice quite possibly would argue that the exception is justified under an exception to the Fourth Amendment, such as emergency or exigent circumstance. *See, e.g.*, Wayne v. U.S., 318 F.2d 205, 212 (D.C. Cir. 1963); U.S. v. Williams, 354 F.3d 497 (6th Cir. 2003). The ACLU coalition letter noted that this dissemination rule applies to communications of a U.S. person, but not to communications of a non-U.S. person who is physically within the United States. For that reason, the latter may have a stronger constitutional claim, because those persons within the U.S. are not protected by the dissemination rule.

information about constitutionally-protected persons, a facial challenge to the CLOUD Act would appear quite weak.

Second, a constitutional claim challenging incidental collection would once again face the obstacle of establishing state action. As discussed in the previous section, the CLOUD Act's focus on searches by foreign governments likely precludes the establishment of state action for purposes of a facial challenge. Establishing state action for an as applied challenge would also be difficult but potentially possible. For instance, an individual might establish facts that the executive agreement is in fact targeting U.S. persons, in violation of the CLOUD Act. Or, an individual might establish facts that minimization requirements or limits on dissemination are being violated.

Even assuming the claimant made it past those obstacles, the mere existence of incidental collection can be legal. As the Foreign Intelligence Surveillance Court of Review (FISCR) stated in 2002: "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[44] The legal question, instead, is whether the volume and type of incidental collection is so significant as to violate the Fourth Amendment. Although one Foreign Intelligence Surveillance Court case from 2011 provides some support for claimants, it would seem difficult to establish that incidental collection under a CLOUD Act executive agreement is significant enough to violate the Fourth Amendment.

The FISCR 2002 decision in *In Re: Sealed Case* supports the view that incidental collection under a CLOUD Act executive agreement would be lawful. In that case, tens of thousands of pieces of evidence were collected under the Foreign Intelligence Surveillance Act ("FISA") without a classic probable cause warrant. The court noted that there is a general "reasonableness" requirement under the Fourth Amendment – evidence may be gathered without a probable cause warrant where the overall regime is "reasonable." Under the CLOUD Act, prosecutors could similarly argue that executive agreements create an overall reasonable system of protections that are sufficient for Fourth Amendment purposes. These protections include targeting and minimization requirements and lawful receipt of foreign government evidence only where there is serious risk of harm. Similar to FISA, and especially if these protections are maintained in practice, a reviewing court might find evidence received from a foreign government to be reasonable and in compliance with the Fourth Amendment despite the absence of a probable cause warrant.

A more recent 2011 FISA decision by Judge Bates provides arguments for the opposite proposition, that incidental collection may trigger a Fourth Amendment violation.[45] Judge Bates' 2011 decision concerned the "Upstream" program under Section 702 of FISA, under which the U.S. government filters the contents of communications that pass through the

[44] *See* [Caption Redacted], No. [Redacted], at 75–76 (quoting *In re Directives Pursuant to SEC. 105b*, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008)).
[45] *See* [Caption Redacted], No. [Redacted] (FISA Ct. Oct. 3, 2011).

Internet backbone.[46] Judge Bates found statutory and constitutional violations in the way that the government was accessing "multi-communication transactions" under the Upstream program.[47] The program was supposed to target only specific "selectors" (such as an email address or phone number). The Court found, however, that between two and ten thousand entirely domestic communications were captured by the Upstream program despite lacking any selectors. It also found tens of thousands of additional communications each year that were sent to or from a constitutionally protected person but did not include a selector.[48] Judge Bates found this number of incidental communications to be a "very large number."[49] He also found the nature of the communications to be highly sensitive. In light of those factual findings, Judge Bates found that the incidental collection violated the Fourth Amendment despite the presence of targeting and minimization procedures.

Although Judge Bates' decision shows the possibility of incidental collection violating the Fourth Amendment, at least three important distinctions make it more likely that incidental collection under the CLOUD Act would be upheld under the Fourth Amendment. First is the scale. In his decision, Judge Bates emphasized the "tens of thousands" of communications per year that "have little or no relationship to the target but [are] protected under the Fourth Amendment."[50] Compared with this quantity of protected communications, the *total* number of requests (both lawful and potentially unlawful) under an executive agreement, and the number of potential violations, would presumably be considerably less.[51] Second, the CLOUD Act mandates that any executive agreement search "shall identify a specific person, account, address, or personal device, or any other specific identifier as the object of the order." That narrowly tailored search contrasts sharply with the large-scale collection under the Upstream program, whose selectors lacked the same specificity. Third, there is also a considerable

---

[46] For details of the Upstream program, see PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (July 2, 2014).

[47] These multi-communications transactions "consist of multiple communications that are packaged and transmitted as a single entity (i.e., the inbox listing of a single communicant is often transmitted by service providers as a single intact stream of bits, even though it represents the leading edge of many individual e-mails)." CHRIS INGLIS & JEFF KOSSEFF, IN DEFENSE OF FAA SECTION 702: AN EXAMINATION OF ITS JUSTIFICATION, OPERATIONAL EMPLOYMENT, AND LEGAL UNDERPINNINGS, HOOVER INST. (2016).

[48] [Caption Redacted], No. [Redacted] at 72 (FISA Ct. Oct. 3, 2011).

[49] *Id.* at 73.

[50] *Id.* at 41.

[51] Major service providers publish transparency reports on government requests for customer data, broken down by category. The scale of all such requests is smaller per year than the number of incidentally collected communications described by Judge Bates. As another limit on quantity of possible violations, the CLOUD Act concerns targeted collection, rather than the large-scale collection of the Upstream program. The CLOUD Act requires that any order issued pursuant to an executive agreement must "identify a specific person, account, address, or personal device, or any other specific identifier." 18 U.S.C. § 2523(b)(4)(D)(ii).

difference in the degree of state action. Judge Bates' decision addressed a collection program conducted by the NSA, a federal agency. By contrast, collection under a CLOUD Act executive agreement is by a foreign government, and therefore generally does not constitute state action under U.S. law.

In conclusion, a facial challenge on incidental collection grounds appears extremely weak in light of the statute's required safeguards. For an as-applied challenge, the claimant would need to show egregious violations of the CLOUD Act. Even then, there are serious doubts about whether the scale and nature of the incidental collection would violate the Fourth Amendment.

III. What Comes Next

While the CLOUD Act's passage was motivated in large part by the desire to moot the *Microsoft Ireland* case before the Supreme Court issued its opinion, the Act's most significant impact will come as executive agreements are negotiated and come into force.[52] If the new U.S.-U.K. CLOUD Act executive agreement survives its congressional review period ending July 8,[53] the CLOUD Act will lift the SCA's blocking statute for U.K. orders subject to the agreement and the current, strict standard of probable cause will no longer apply for British requests for evidence about non-U.S. persons located outside the U.S.[54] While the CLOUD Act requires that these requests comply with significant procedural and specific privacy safeguards, admittedly that is not equivalent to the Constitution's probable cause standard – a major criticism by privacy and human rights advocates. To address these criticisms the U.S.-U.K. executive agreement includes several new safeguards including ones not included in the CLOUD Act itself.[55] These significant new safeguards, include:

- The specification that orders subject to the agreement must be reviewed and certified as lawful by a designated authority;

[52] To date, the CLOUD Act's codification of the scope of U.S. law enforcement's authority to access electronic evidence stored outside the U.S. has led to critique and discussion, particularly from European Union Member States. While this is an important topic, and one which both authors address separately as part of our work with the Cross-Border Data Forum, this aspect of the CLOUD Act is not the focus of our legal and constitutional analysis here. *See* Sophie in 't Veld, *Privacy Platform: The CLOUD Act and e-Evidence: "America first" or GDPR first? Challenges of Transatlantic Access to e-Evidence in Law Enforcement*, STERK EUROPA SOPHIE (Jan. 17, 2019); Theodore Christakis, *Transfer of EU Personal Data to U.S. Law Enforcement Authorities after the CLOUD Act: Is there a Conflict with the GDPR?*, CROSS-BORDER DATA FORUM (Jun. 13, 2019); *see, e.g.*, Peter Swire & Jennifer Daskal, *Frequently Asked Questions about the U.S. CLOUD Act*, CROSS-BORDER DATA FORUM (Apr. 16, 2019); Justin Hemmings & Nathan Swire, *Lawfare – Why the CLOUD Act is Not a Tool for Theft of Trade Secrets*, CROSS-BORDER DATA FORUM (Apr. 24, 2019).

[53] Justin Hemmings, CLOUD Act Executive Agreement Certified to Congress, After a Delay, CROSS-BORDER DATA FORUM (Jan. 21, 2020).

[54] Letter from Access Now et al., *supra* note 9.

[55] Peter Swire & Justin Hemmings, *Recommendations for the Potential U.S.-U.K. Executive Agreement Under the CLOUD Act*, LAWFARE (Sep. 13, 2018).

- Providers who receive orders can go back to the designated authority if and when they have specific concerns;
- The agreement allows the U.K. to refuse evidence sharing with the U.S. if the latter is seeking the death penalty in a particular case, and the U.S. can similarly veto evidence sharing where the U.K.'s case raises free expression concerns;
- When seeking the data of someone reasonably believed to be in a third country, the agreement requires notification to the third country government where the target is located unless doing so would be detrimental to the investigation, operational or national security, or human rights;
- The U.K. must enact minimization and targeting procedures, and any changes to those procedures must be approved by the U.S. prior to implementation;
- The U.S. may not target U.K. persons located within the U.K. (though they may target UK citizens and lawful permanent residents who are not physically located in the U.K.);
- Providers can notify their home government about any objectionable requests;
- The agreement defines a "serious crime" as one with a maximum punishment of three or more years of incarceration; and
- The agreement specifies the possibility of issuing preservation orders for content, non-content, and subscriber data.[56]

Now that the agreement has been signed, it will go to the Congress, which has 180 days to scrutinize the agreement. If Congress takes no action, the agreement will then enter into force.

Ultimately, it seems challenges to the CLOUD Act are most likely to arise once an executive agreement is in force. Parties will likely closely scrutinize the Congressional review process to make sure that the CLOUD Act's requirements for qualifying foreign entities are met, and that Congress does not merely rubber stamp a determination from the Attorney General and Secretary of State.[57] Once implemented, an executive agreement will also offer as-applied fact patterns that could "stress test" the constitutionality of the CLOUD Act, with possible claims by electronic service providers and defense attorneys. Yet, for now, it seems the Act rests on firm, if untested, constitutional grounds.

[56] Jennifer Daskal and Peter Swire, *The U.K.-U.S. CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019).
[57] *See* 18 U.S.C. § 2523(d).

About the Authors

Peter Swire is the Elizabeth and Thomas Holder Chair and Professor of Law and Ethics at the Georgia Institute of Technology Scheller College of Business. He is a Senior Fellow with the Future of Privacy Forum, a Member with the National Academy of Sciences & Engineering Forum on Cyber Resilience, and Research Director for the Cross-Border Data Forum. He is also Senior Counsel with Alston & Bird LLP. In 2018 Swire was named an Andrew Carnegie Fellow for his project on cross-border data flows. Under President Obama, Swire served as Special Assistant to the President for Economic Policy and served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Under President Clinton Swire was the Chief Counselor for Privacy in the U.S. Office of Management and Budget, the first person to have U.S. government-wide responsibility for privacy protection. A prolific writer, Swire is the author of six books and numerous scholarly papers and has testified often before Congress. Swire graduated from Yale Law School where he was an editor of the *Yale Law Journal*.

Justin Hemmings is a Research Faculty Member at the Georgia Institute of Technology Scheller College of Business and a Project Attorney at Alston & Bird LLP where he engages in legal and policy issues and practices concerning privacy and cybersecurity. He and Peter Swire co-authored the 2017 *NYU Annual Survey of American Law* article "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program," which proposed the executive agreement approach that was later codified in Section 5 of the CLOUD Act. Hemmings received his J.D. from American University Washington College of Law.

About the American Constitution Society

The American Constitution Society (ACS) believes that law should be a force to improve the lives of all people. ACS works for positive change by shaping debate on vitally important legal and constitutional issues through development and promotion of high-impact ideas to opinion leaders and the media; by building networks of lawyers, law students, judges and policymakers dedicated to those ideas; and by countering the activist conservative legal movement that has sought to erode our enduring constitutional values. By bringing together powerful, relevant ideas and passionate, talented people, ACS makes a difference in the constitutional, legal and public policy debates that shape our democracy.