Cross-Border Law Enforcement Access to E-Evidence: The State of the Playing Field After The Passage of the U.S. CLOUD Act

By Zarine Kharazian and Bruce Zagaris

Governments need access to evidence to investigate and prosecute crimes. Increasingly, that evidence exists in the form of e-evidence – electronic communications and metadata – stored on (most often U.S.) tech company servers across the world. Thus far, the primary means for foreign governments to obtain data stored in another country is via a Mutual Legal Assistance Treaty (MLAT). An MLAT facilitates assistance between two or more countries’ law enforcement authorities on duties that range from obtaining witness testimony to executing search warrants.2

In recent years, criminals have increasingly turned to the Internet to communicate with others and store their data or proceeds of crime. As a result, MLAT requests have increased steadily. In 2000, the United States sent over 500 MLAT requests and received over 1,500.3 By 2014, those numbers had roughly doubled, with the United States sending over 1,000 requests and receiving 3,250. The increase has put a noticeable strain on an already cumbersome process, and foreign governments have grown increasingly frustrated in turn.4

In response, the United States and foreign governments have begun to enact legislation to facilitate the law enforcement agencies’ access to data stored across borders. This article provides some background on the United States’ approach to the issue, and then moves to discuss similar legislation from other countries.

Background: The CLOUD Act

On March 23, 2018, President Donald Trump signed the 2018 Omnibus Spending Bill into law. Tacked on to the spending bill was the Clarifying Lawful Overseas Use of Data (CLOUD) Act, a controversial piece of legislation with substantial implications for data privacy and security. Much to the ire of privacy and civil liberties groups like the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU), Congress appended the CLOUD Act to the spending bill at the last minute, without conducting an independent hearing or vote on its provisions.

The CLOUD Act clarifies that the Stored Communications Act’s (SCA) rules governing U.S. law-enforcement agents’ access to content and non-content information, including the provision requiring that law enforcement obtain a warrant before demanding that email providers turn over private email content,5 generally apply to data that is stored outside the United States as well. The CLOUD Act authorizes the United States government to enter into reciprocal data-sharing agreements, called “executive agreements” with foreign governments to facilitate the exchange of electronic data to aid in criminal investigations. The international agreements envisioned by the CLOUD Act, will require the U.S. and participating foreign governments to remove lift restrictions on providers' compliance with other countries' legal requests, introducing a measure of clarity for providers who had increasingly been caught in the middle of irreconcilable legal obligations imposed by different jurisdictions.

The Act has two parts: the first governs U.S. law enforcement’s access to data stored abroad by electronic communications providers, and the second governs foreign law enforcement’s access to data stored in the United States. In both cases, the requesting government may compel a third-party electronic communications provider, such as Microsoft, to disclose information about or the contents of a communication pertaining to an individual customer, if the requesting government has an executive agreement in place with the country in which the data is stored. The CLOUD Act provides for a new, formal process for providers to challenge U.S. law-enforcement demands for user data both in a country in which there is a CLOUD Act executive agreement and in countries where there are no agreements. Additionally, the Act allows providers to inform the foreign government of the law-enforcement request so that the foreign government can object directly to the U.S. government if it wishes.

---

3 Id.
4 Id.
With respect to foreign requests for electronic information to the U.S., the CLOUD Act aims to streamline this process by providing that when the U.S. enters into an Executive Agreement with a qualifying foreign country, the foreign law-enforcement requests for data may be responded to directly by providers. In essence, the Executive Agreements preauthorize law-enforcement requests from certain foreign countries.

Human rights and privacy organizations like the ACLU, EFF, and Amnesty International have denounced the executive agreement mechanism for what they see as providing unfettered access to U.S.-held data to foreign governments. Other critics have been alarmed about the provisions in the act that grant U.S. law enforcement access to data stored abroad, with some suggesting that the CLOUD Act directly conflicts with European data protection directives, notably the 2018 General Data Protection Regulation (GDPR).

The EU e-Evidence Initiative

On April 17, 2018, the European Commission proposed a regulation (on European Production and Preservation Orders for electronic evidence in criminal matters) and a directive (Laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings).

The regulation introduced two instruments – a European Production Order and a European Preservation Order. The former allows an E.U. Member State’s judicial authority to compel a service provider in another state to preserve specific data while the data request is being processed. Both instruments are intended to significantly speed up the data request process, introduce safeguards for the protection of individual rights, and provide legal clarity for service providers regarding requests for electronic communications.6

The directive aims to harmonize disparate national frameworks within the E.U. regarding obligations imposed on service providers to provide access to data. It does so by requiring service providers in the E.U. to designate a legal representative to handle requests for access to electronic data from law enforcement.7

UK Overseas Production Act

In the U.K, a separate proposal regarding law enforcement access to e-evidence is making its way through Parliament. The Overseas Production Act (OPA) would allow law enforcement agencies to request electronic data directly from service providers, thereby bypassing the cumbersome mutual legal assistance process. Like the CLOUD Act, the current version of the bill sets forth restrictions on the type of data covered under the OPA. For example, the data must be of “substantial value” to the ongoing investigation, and the production of the data must serve the public interest.8 The bill also requires that an international agreement already be in place between the requesting country and the recipient country, similar to the executive agreements framework of the CLOUD Act.9

The Chinese regulation governing collection and transfer of data in criminal investigations

China is also in the process of establishing its own guidelines. On September 20, 2016, the Supreme People’s Court of the Supreme People’s Procuratorate (China’s prosecutorial agency) released the Chinese regulation governing collection and transfer of data in criminal investigations.

The Guidelines define domestic operation as providing products or services within China. A foreign network operator that while not registered in China provides products or services to customers in China is engaged in domestic operation and hence will be subject to China’s cross-border data transfer requirements. China’s Cybersecurity law became effective last year. It requires critical information infrastructure operators (CIIOs) to store personal information and important data collected and generated within the territory of the PRC.10

---


10. See Chinese regulation governing collection and transfer of data in criminal investigations, released by September 20, 2016 the Supreme People’s Court, Supreme People’s Procuratorate (China’s prosecutor) http://www.spp.gov.cn/xwfbh/wsfbh/2
The Guidelines require a regulated company to conduct a security assessment of the system it will use to transfer the data. No new security assessment is needed for data transfers involving same parties, scope, type, etc. within a period of one year.\(^1\) The regulations seem to authorize the unilateral extraction of data concerning anyone (or any company) being investigated under Chinese criminal law from servers and hard drives located outside of China.”\(^2\) In particular, Article 9 of the regulations authorize Chinese law enforcement officials to obtain data from storage media (such as servers and hard drives) located outside of mainland China. They may obtain this data through the Internet or via “remote network inspections.” Hence, China is also developing compulsory measures to gain access to electronic data. In a blog post published by the Council of Foreign Relations, argues that, “Whether the U.S. government compels a company to hand over data or the Chinese authorities simply take it, the intent and effect are the same.”\(^3\)

**Analysis**

The CLOUD Act and legislation by the EU and other countries will put more order in the ways in which governments seek electronic evidence in cross-border criminal cases. However, because of the differences in privacy and fundamental laws regarding privacy, as well as the range of policies on cybercrime and cybersecurity, the international seems to be in the beginning stages of regulating access to electronic evidence, and doing so in a way that balances the needs of law enforcement and regulators to access such information with the privacy and fundamental rights of other stakeholders.

**The CLOUD Act: Arguments For and Against**\(^4\)

**By Zarine Kharazian**

On February 27, 2018, the United States Supreme Court heard oral arguments in the seminal data privacy case of the term, United States v. Microsoft Corp. At issue in the case is whether the warrant provisions of the Stored Communications Act (SCA) apply extraterritorially, such that they compel Microsoft, an electronic service provider to produce private electronic communications stored on servers in Ireland for the United States government. Microsoft argues that the SCA does not apply to electronic communications stored in overseas data centers; the U.S. government begs to differ.

The justices, for their part, expressed a range of diverging sympathies, with the conservative justices leaning more heavily in favor of the government. They all seemed to agree, however, on one point: our increasingly networked world has rendered the SCA woefully outdated. When Congress enacted the Stored Communications Act in 1986, Justice Ruth Bader Ginsburg observed, “no one ever heard of clouds. This kind of storage didn’t exist.”\(^5\)

The justices also suggested, however, that it should be the job of Congress, not the Court, to modernize the legislation for the 21st century. “It would be good if Congress enacted legislation that modernized this,” Justice Alito noted. Justice Sotomayor, wary of the Court wading into “international problems,” challenged, "[w]hy shouldn't we leave the status quo as it is and let Congress pass a bill in this new age?"\(^6\)

The justices got what they had hoped for; on March 23, 2018, Congress enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act. Shortly thereafter, the Department of Justice and Microsoft both filed motions to dismiss the closely-watched data privacy case as moot. The two parties agreed that the recently-enacted legislation resolves the “live case or controversy” with respect to the

---

1. Id.
2. Id.
3. Susan Hennessey and Christopher Mirasola, Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?, LAWFAREBLOG.COM, Mar. 27, 2017
4. Lincoln Davidson, China and the United States Have an Eerily Similar Approach to
5. Id.
question presented. On April 17, 2018, the Court released an unsigned opinion that dismissed the case as moot on the grounds that “no live dispute remains between the parties.”17

Although the CLOUD Act passed with bipartisan support, it remains highly controversial in technology and privacy circles. Big technology companies, such as Google and Microsoft, generally support it, while privacy advocates and human rights groups, such as the American Civil Liberties Union (ACLU) and Human Rights Watch (HRW), oppose it. In this article, I identify the CLOUD Act’s key provisions, outline the contours of the existing debate, and argue that, on balance, the CLOUD Act solves more problems than it creates.

The CLOUD Act’s Key Provisions

The CLOUD Act facilitates and streamlines law enforcement access to data stored across borders. The act has two parts. The first part governs U.S. law enforcement access to data stored abroad. This portion of the act amends the Stored Communications Act to state as follows:

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.18

Here, the Act clarifies that U.S. electronic providers must comply with an order issued under the SCA to disclose the contents of an electronic communication irrespective of whether the data is located within or outside the United States. In other words, a warrant issued under the SCA does have extraterritorial reach.

The second part of the CLOUD Act consists of provisions governing foreign governments’ access to U.S.-held data. In particular, the act authorizes the president of the United States to enter into reciprocal data-sharing “executive agreements” with foreign governments.

In order to benefit from an executive agreement, however, foreign governments must meet certain standards with regards to human rights and the rule of law. Among other requirements, the government in question must:

1) Have domestic law that “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;” and
2) Have instituted “appropriate procedures to minimize the acquisition, retention, and dissemination of information concerning United States persons subject to the agreement;” as well as that;
3) The government adopts procedures that guard against targeting, either direct or indirect, of a U.S. citizen or person located in the United States.19

Furthermore, the act specifies further criteria for what constitutes a qualifying order for the disclosure of U.S.-held data to a foreign government. In particular, the order must:

1) Be for the purpose of “obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism;”
2) Identify a “specific person” or other “specific identifier” as the object of the order;
3) Comply with the requesting country’s domestic law;
4) Be subject to independent oversight by a judge, court, magistrate, or other legal authority; among other qualifications.20

The act also includes a provision requiring the qualifying foreign government to submit to “periodic review of compliance” with the terms of the agreement, to be conducted by U.S. officials.21

---

19 Id.
20 Id.
21 Id.
The State of the Debate: Does the CLOUD Act Help or Hinder Human Rights?

In an initial essay posted on Lawfare, Jennifer Daskal and Peter Swire argued that the CLOUD Act will enhance, rather than dilute, privacy and human rights protections on balance. They note that the status quo for requesting evidentiary data across borders – the Mutual Legal Assistance Treaty process – is a cumbersome bureaucratic channel ill-equipped for the sheer number of cross border data requests currently in the system. As a result, countries are growing more and more frustrated with the MLAT process, which they view as not only cumbersome, but “imperialistic,” since it often requires getting a warrant from a U.S.-based judge even if the data requested concerns a local criminal investigation.

Countries are thus turning to alternative measures to bypass the MLAT system, such as data localization laws that require that data be stored within the country. Data localization laws have been accused by critics of veiling anti-democratic motivations on the part of the instituting government – by allowing for closer surveillance and identification of local political dissidents, for example. Furthermore, data localization laws lead to data decentralization, which in turn leads to multiple points of vulnerability in data providers’ security and privacy infrastructure.

Daskal and Swire also praise the CLOUD Act’s periodic compliance review requirement as a novel opportunity for the U.S. to monitor how foreign governments use the data and guard against abuse.

Neema Singh Guliani from the ACLU and Naureen Shah from Amnesty International counter in a response essay that the CLOUD Act puts the privacy and security of individuals, particularly human rights activists, at risk. The very premise of the current CLOUD Act, they write, “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.” Guliani and Shah argue that the CLOUD Act has inadequate safeguards for wide range of scenarios, such as when a country experiences a “rapid deterioration in human rights,” like Turkey did in mid-2016 following a coup attempt.

Guliani and Shah also criticize the act for a lack of clarity on certain points. They note that, while the act requires qualifying governments to demonstrate a respect for “international universal human rights,” it does not define the term. They also criticize the act for requiring a foreign government to demonstrate respect for free expression, but failing to state the legal standard – United States, international, or domestic – under which the term is defined.

Governments need access to evidence to investigate and prosecute crimes. Increasingly, that evidence exists in the form of e-evidence – electronic communications and metadata – stored on U.S. tech company servers across the world. Thus far, the primary means for foreign governments to obtain data from U.S. companies is via a bilateral or multilateral MLAT treaty. An MLAT facilitates assistance between two or more countries’ law enforcement authorities on duties that range from obtaining witness testimony to executing search warrants.

In recent years, criminals have increasingly turned to the Internet to communicate with others and store their data or proceeds of crime. As a result, MLAT requests have increased steadily. In 2000, the United States sent over 500 MLAT requests and received over 1,500. By 2014, those numbers had roughly doubled, with the U.S sending over 1,000 requests and receiving 3,250. The increase has put a noticeable strain on an already cumbersome process, and foreign governments have grown increasingly frustrated in turn.


23 Id.

24 Id.

25 Id.


27 Id.

The CLOUD Act resolves two cardinal problems with the status quo with regards to foreign governments’ access to data held by U.S. providers. First, it allows a foreign government to bypass the inefficient MLAT process when seeking access to e-evidence held by a U.S. service provider, provided the foreign government already has an executive agreement in place with the United States. In allowing a qualifying government to submit its request directly to the U.S. service provider, the CLOUD Act relieves some of the burden on the inundated MLAT system. Second, it removes the requirement that U.S. legal standards be met for what is often a foreign local criminal investigation. Instead, the CLOUD Act relies on both the foreign government’s own domestic law and the international normative standards set forth in the act. In resolving these problems, the CLOUD Act removes two main incentives that foreign governments have had until now to enact alternative measures, such as expanding their surveillance powers or requiring data localization policies.

The CLOUD Act is certainly not perfect. Critics have raised legitimate concerns regarding the possible politicization of the process. “Tucked away in the omnibus spending bill is a provision that allows Trump, and any future president, to share Americans’ private emails and other information with countries he personally likes. That means he can strike deals with Russia or Turkey with nearly zero congressional involvement and no oversight by U.S. courts,” Oregon Democratic Senator Ron Wyden has said of the bill.\(^9\) There is an important role for privacy advocates and human rights group to play to pressure the U.S. government to release to the public the rationale for why an executive agreement with a particular country is approved, as well as the criteria for the mandated periodic compliance reviews. On balance, however, the CLOUD Act is a welcome, albeit overdue, step in the right direction.

**European Commission Recommends Negotiating a Treaty with U.S. on Access to Electronic Evidence**

*Michael Plachta*

On February 5, 2019, the European Commission published its recommendations for the Council to engage in two international negotiations on cross-border rules to obtain electronic evidence.

Following up on the European Council Conclusions from October 2018, the Commission presented two negotiating mandates, one for negotiations with the United States and one on the Second Additional Protocol to the Council of Europe “Budapest” Convention on Cybercrime. Both mandates, which need to be approved by the Council of the European Union, include specific safeguards on data protection, privacy, and procedural rights of individuals.

More than half of all criminal investigations today require access to cross-border electronic evidence. Electronic evidence is needed in around 85% of criminal investigations, and in two-thirds of these investigations there is a need to obtain evidence from online service providers based in another jurisdiction. The number of requests to the main online service providers grew by 84% in the period between 2013 and 2018. These types of data are essential in criminal investigations to identify a person or to obtain information about their activities.\(^3\)

In the April 2015 European Agenda on Security, the Commission committed to review obstacles to criminal investigations. Following the tragic events in Brussels on March 22, 2016, EU Ministers for Justice and Home Affairs prioritized passing measures to secure and obtain digital evidence more efficiently and effectively.\(^2\)

The issue has since been discussed several times by EU Ministers. In its resolution adopted on October 3, 2017, the European Parliament stressed that cyber-resilience is key in preventing cybercrime and should therefore be given the highest priority.\(^3\) In December 2017, the Commission


---

* Professor Plachta specializes in criminal law and international criminal law. He has authored numerous publications on a wide range of issues concerning law enforcement and international cooperation in criminal matters. He currently teaches criminal law and European criminal law at the University of Security in Poznan, Poland.


presented an intermediary report on the implementation of the Council conclusions. In April 2018 the Commission proposed new rules for cross-border access to electronic evidence.\(^{34}\) In October 2018, European Leaders called on the Commission to urgently submit negotiating mandates for the international agreements on electronic evidence. It has also been discussed at recent EU-U.S. Justice and Home Affairs Ministerial meetings.

With an increasing number of investigations needing access to electronic evidence, such as e-mails or documents located on the Cloud, in April 2018 the Commission proposed new rules making it easier for police and judicial authorities to follow leads online and across borders. Given that a number of service providers are based outside of the EU, present mandates complete the new rules to ensure greater cooperation at the international level.

It is noteworthy that the Council of Europe decided to draft an additional protocol to the Budapest Convention of Cybercrime in order to lay down provisions for a more simplified mutual legal assistance (MLA) regime and for provisions allowing for direct cooperation with service providers in other jurisdictions.\(^{35}\)

One of the main recipients of MLA requests from EU Member States for access to electronic evidence is the United States. An agreement on MLA was signed on June 25, 2003 and entered into force on February 1, 2010. A first joint review of the agreement took place in 2016. Its outcome was to encourage Member States to cooperate directly with U.S. service providers in order to secure and obtain electronic evidence more quickly and effectively.\(^{36}\)

Direct cooperation with U.S. service providers has developed as an alternative channel to judicial cooperation. It is limited to non-content data and is voluntary from the perspective of U.S. law. In practical terms, the public authorities of the EU Member State directly contact a service provider in the United States with requests pursuant to national rules of criminal procedure to which the service provider has access, typically data on a user of the services it provides.\(^{37}\)

Major service providers holding relevant evidence for criminal investigations operate under U.S. jurisdiction. The Stored Communications Act of 1986 prohibited the disclosure of content data, whereas non-content data can be provided on a voluntary basis. The United States CLOUD Act, adopted by U.S. Congress on March 23, 2018, clarifies through an amendment of the Stored Communications Act of 1986 that U.S. service providers are obliged to comply with U.S. orders to disclose content and non-content data, regardless of where such data is stored, including in the European Union. The CLOUD Act also allows the conclusion of executive agreements with foreign governments, on the basis of which U.S. service providers would be able to deliver content data directly to these foreign governments.

An EU-U.S. Agreement would complement the objective and the effectiveness of the e-evidence proposals, in particular when it comes to content data held by U.S. service providers in the United States. It would allow direct cooperation with a service provider by creating a more efficient legal framework for judicial authorities as EU practitioners currently face difficulties in obtaining content data through MLA requests.\(^{38}\)

As regards non-content data, due to the growing number of MLA requests addressed to the United States, the U.S. authorities have encouraged EU law enforcement and judicial authorities to request non-content data from U.S. service providers directly, and U.S. law allows but does not require U.S.-based service providers to respond to such requests. An EU-U.S. Agreement would provide more certainty, clear procedural safeguards, and reduce fragmentation for EU authorities to access non-content data held by U.S. service providers. It would also allow for reciprocal access by U.S. authorities to data held by EU service providers.\(^{39}\)

According to the Commission, the agreement should be without prejudice to other existing


\(^{36}\) Review of the 2010 EU-U.S. Mutual Assistance Agreement, 7 April 2016, 7405/16.


\(^{39}\) Id., at 5.
international agreements on judicial cooperation in criminal matters between authorities, such as the EU-U.S. Mutual Legal Assistance Agreement. The agreement should, in the bilateral relations between the U.S. and the EU, take precedence over any agreement or arrangement reached in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime.  

The negotiating instruction is set in an annex to the Commission’s Recommendation and covers objectives of the agreement, its nature and scope, safeguards, and governance of the agreement. The Commission should, in the course of the negotiations, aim to achieve the specific objectives set out in detail in an annex, while ensuring that the outcome of the negotiations is compatible with the Union’s internal rules on electronic evidence, including as they evolve in the legislative procedure by the Union co-legislators and eventually in their final adopted form.

Specifically, the negotiating mandate proposed by the Commission aims to: (i) ensure timely access to electronic evidence for law enforcement authorities in the EU and the U.S. by shortening the time period for supplying the requested data to 10 days (currently it takes on average 10 months); (ii) address legal conflicts by setting out definitions and types of data covered, clarifying legal obligations and ensuring reciprocal rights for all parties; (iii) guarantee strong safeguards on data protection, privacy, and procedural rights in full respect of fundamental rights and the principles of necessity and proportionality.

The Budapest Convention is the centerpiece of international cooperation against cybercrime providing a comprehensive framework for cooperation for over 60 countries. The Second Additional Protocol, once in place, will further strengthen this international cooperation including on obtaining access to electronic evidence, enhancing mutual legal assistance, and setting up joint investigations.

The Commission has proposed a mandate to participate in those negotiations on behalf of the European Union and its Members to ensure: (i) compatibility of the Protocol with current and future EU law, including in the area of cross-border access to electronic evidence; (ii) enhanced international cooperation through more effective mutual legal assistance, including simplified requests, and setting up joint investigations teams; (iii) direct cooperation of law enforcement with service providers in other jurisdictions; (iv) stronger safeguards for the protection of personal data and national practices on cross-border access to data.

In view of the absence of provisions for authorities to access data without the help of an intermediary (“direct access”) in the European Commission’s e-evidence proposals, any use of those measures can only be based on national law. Where the Second Additional Protocol may include provisions in relation to the “Extension of searches and access based on credentials” and “Investigative Techniques”, the main aim should be to pursue stronger safeguards for such cross-border direct access to data to ensure the protection of fundamental rights and freedoms of EU citizens, including privacy and personal data protection.

The two recommendations – to open negotiations with the United States and to participate in the negotiations of the Second Additional Protocol to the Council of Europe Convention on Cybercrime – are being adopted by the Commission at the same time. While the two processes will progress at a different pace, they address inter-linked issues and commitments taken in one negotiation may have a direct impact on other strands of negotiations.

U.S. Department of Justice Publishes White Paper on the Cloud Act

By Bruce Zagaris

On April 10, 2019 the U.S. Department of Justice announced the public release of a white paper on the Clarifying Lawful Overseas Use of Data Act (CLOUD Act).

Id. at 7.


Id., at 6.

Id., at 7.

Michael Plachta, supra note 5.

March 2018, the Act updates the legal framework for how law enforcement authorities may request electronic evidence required to protect public safety from service providers while respecting privacy and foreign sovereignty.

Deputy Attorney General Rod Rosenstein promises the DOJ will be proactive in working, both in the U.S. and abroad, to promote greater understanding and appreciation of what the CLOUD Act does.

*The CLOUD Act Executive Agreements*

The CLOUD Act has two distinct parts. First, the Act authorizes the U.S. to enter into bilateral agreements to facilitate the ability of trusted foreign partners to obtain the electronic evidence they required to fight serious crime. To qualify under the Act, a partner country must adhere to baseline rule-of-law, privacy, and civil liberties protections. Through bilateral agreements, each country would agree to lower the legal barriers that prevent their communication service providers from complying with qualifying lawful orders for electronic data issued by the other country. By lowering legal barriers, each country could serve its legal process, such as search warrants, directly on the providers of the other country, significantly increasing the speed and efficiency compared with existing methods of transferring electronic evidence.

Both signatories would be able to submit orders for electronic evidence required to combat serious crime directly to CSPs, without involving the other government and without fear of conflict with the U.S. or the other signatory’s law. Many countries have said that the MLAT process is not fast enough to provide timely access to electronic data held by global CSPs based in the U.S. for purposes of their criminal investigations.

Without the CLOUD Act agreement, many U.S.-based global CSPs will not disclose electronic data directly to foreign investigating authorities, even if they are served with an order by the foreign authority because the companies are concerned about potential restrictions in U.S. law on disclosure of electronic data and liability if they comply with the foreign orders. The potential for conflict of laws exists even when the request from the investigating country involves only communications between non-U.S. persons located abroad and concerns criminal activities occurring entirely outside the U.S.

The only legal effect of a CLOUD agreement is to eliminate the legal conflict for qualifying orders. Since the U.S. currently receives many more requests for electronic data than it submits to other countries, the U.S. expects the CLOUD Act will have a more dramatic (and beneficial) impact on foreign requests to the U.S. than on U.S. requests to foreign partners.

The CLOUD Act requires that the agreements include many provisions protecting privacy and civil liberties. Orders requesting data must be lawfully obtained under the domestic system of the country seeking the data; must target specific individuals or accounts; must have a reasonable justification based on articulable and credible facts, particularity, legality, and serenity; and must be subject to review or oversight by an independent authority, such as a judge or magistrate. Bulk collection is not permitted. Foreign orders cannot target U.S. persons or persons in the U.S. Agreements may be used only to obtain information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism.

A CLOUD Act agreement would not be the exclusive mechanism for either party to the agreement to obtain electronic data; other mechanisms such as MLATs or domestic orders outside the agreement would remain available. However, CLOUD agreements will reduce the burden on the MLAT system, and remove potential legal conflicts that might otherwise be posed by domestic enforcement of orders, by allowing CSPs to respond directly to covered foreign orders without fear of a conflict between the two parties’ laws.

CLOUD Agreements will not address challenges posed to law enforcement by end-to-end encryption, where decryption capability is limited to the end user.

*Ensuring Lawful Access to Data*

Second, the CLOUD Act sets forth in U.S. law the principle, longstanding in both the U.S. and many foreign countries, that a company subject to U.S. jurisdiction can be required to produce data within its custody and control, regardless of where it chooses to store that data at any point in time. This was a key issue in *United States v. Microsoft Corporation*, No. 17-2, a case argued before the

*White Paper April 2019  
The DOJ compiled the white paper with the input of components across the DOJ, including attorneys from the Criminal Division and the National Security Division. The white paper discusses the interests and concerns that prompted the enactment of the CLOUD Act and provides a distillation of the effect, scope, and implications of the Act, as well as answers to frequently asked questions.

The DOJ white paper has 28 Frequently Asked Questions at the end. For instance, FAQ 7 clarifies that the legal process by a country under a CLOUD Act agreement need not have to confirm to the requirements of U.S. law, but only to the requirements of that country’s domestic law for the data sought.

Analysis

On April 5, 2019, Deputy Assistant Attorney General Richard W. Downing delivered remarks at the Academy of European Law Conference on “Prospects for Transatlantic Cooperation on the Transfer of Electronic Evidence to Promote Public Safety” in London, United Kingdom. Downing stated a natural reaction from national governments as they seek to protect the safety and privacy of their citizens is to create new restrictions on other countries’ access — new “blocking statutes.” The temptation is to unilaterally increase pressure on companies to disclose evidence. The temptation is to insist that data be stored within a country’s borders to make access easier. Such reactions run the risk of causing conflicts and paralysis that will hurt us all.

Since it was enacted last March 2018, Downing said the CLOUD Act has, unfortunately, been the subject of many misconceptions, and is viewed by some with suspicion. That may not be surprising, given the complexity and technicality of some of the issues involved. Downing continued that “one particularly inaccurate statement about the Act being made in some circles is that it is a U.S.-centric law designed solely to serve U.S. interests and U.S. needs.” Downing said that in fact the impetus for the CLOUD Act came from our foreign law enforcement partners, who expressed a need for increased speed in obtaining evidence held by U.S. providers — evidence which is normally obtained through the Mutual Legal Assistance Treaty – or “MLA” – process.

An issue may be that the U.S. Attorney must certify that the partner country has in its laws, and implements in practice, robust, substantive, and procedural protections for privacy and civil liberties, based on very broad factors. Each of the factors requires the U.S. Attorney to apply international and comparative law to six large areas of the partner country’s laws. One can say that in the last few years, the U.S. government’s adherence to these broad
factors, such as the respect for the rule of law and principles of nondiscrimination, as well as adherence to international human rights obligations has fallen. Hence, while on paper the requirements for entering a CLOUD Act agreement with the U.S. seem vanilla, even U.S. allies may have a concern in an era where there are heightened controversy about the use of extraterritorial jurisdiction, overlapping jurisdiction for issues concerning the Internet, intelligence gathering, the political use of law, and disagreements about the proper application of international human rights.