REMARKS OF DEPUTY ASSISTANT ATTORNEY GENERAL

RICHARD W. DOWNING

At the International Symposium on Cybercrime Response

September 13, 2023

Remarks as prepared for delivery

At the U.S. Department of Justice, I serve as the Deputy Assistant Attorney General in the Criminal Division overseeing cybercrime, intellectual property offenses, and child exploitation crimes. In this role, I have seen criminal investigations turn increasingly transnational, with victims, witnesses, perpetrators, and evidence located across the globe. Working efficiently and collaboratively with foreign law enforcement partners has proven to be an absolute necessity. Dismantling major criminal networks cannot be accomplished by one country; it depends increasingly on international cooperation amongst law enforcement partners.

These are challenges that are compounded by dramatic advances in technology and the exponential rise of electronic evidence. And such challenges are compounded still further by the unprecedented proliferation of platforms and the globalization of companies. Often electronic evidence is held by companies with transnational operations – with customers, company offices, and data storage facilities located in many different countries. These companies and the data they control may be subject to more than one country's laws, creating conflicting legal obligations when a company receives an order from the government in one country requiring the disclosure of data but the laws of another country restrict disclosure of that same data.

These potential legal conflicts present significant challenges to governments' ability to acquire electronic evidence that may be vital to pursuing criminal investigations in a timely, efficient manner. Such conflicts pose serious problems for law enforcement agencies seeking data and can have a direct impact on public safety.

The Current Landscape

There are existing channels that address some of these problems. The system of agreements called Mutual Legal Assistance Treaties or MLATs permits law enforcement agencies in one country to seek the assistance of foreign counterparts who can obtain the data. The foreign counterpart reviews a request under its own legal standards and may seek a court order under its law to obtain the data. If the order is granted, the foreign government obtains the data and transmits it to the requesting government. This is the primary mechanism for facilitating

international law enforcement cooperation, but this process has many steps, and depending on the country and the complexity of the request, can take many months or even years to complete for a single request for data. The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world.

Another critical piece of our toolkit is the Council of Europe Convention on Cybercrime, commonly known as the "Budapest Convention." The Budapest Convention remains the primary, and currently the only, multi-lateral international treaty that addresses cybercrime and electronic evidence. Countries who are party to the Convention are required to criminalize a common set of computer-related crimes, and the Convention provides a platform for transnational law enforcement cooperation in investigations, evidence sharing, and extradition.

While it's a Council of Europe instrument, it is open to all countries. Currently 68 countries – from every corner of the globe – are party to the Budapest Convention. It is our vision that every country serious about fighting cybercrime should become party to the Budapest Convention, as it strikes the right balance between, on the one hand, imposing obligations on nations to have robust laws and capabilities and, on the other, providing the flexibility necessary to be implemented by countries with different legal systems. We are excited to see the Republic of Korea's interest and its recent steps to join the Budapest Convention.

Even though the Budapest Convention opened for signature over twenty years ago, it is still vital today and changing to meet new challenges in cybercrime and electronic evidence. I was very proud to sign the Second Additional Protocol of the Budapest Convention on behalf of the United States in May of last year. The new protocol provides new pathways to obtain basic subscriber information and even, in some cases, traffic data, from providers located in other countries. There is also a provision to provide a clear pathway to request content and other stored data in emergencies.

The Second Additional Protocol will further accelerate cooperation among parties to protect our citizens and hold criminals accountable. This Protocol is specifically designed to help our law enforcement authorities obtain access to evidence held in other countries, while ensuring that these transfers are subject to appropriate protections and safeguards.

The CLOUD Act as a New Paradigm for International Law Enforcement Cooperation

The international community continues to struggle with the critical question of how to provide law enforcement agencies efficient and effective access to electronic evidence needed to protect public safety while preserving respect for sovereignty and privacy.

There is a widespread understanding that countries need the domestic authority to compel providers within their jurisdictions to produce electronic evidence within the providers' possession, custody, or control, regardless of where the providers might choose to store that

data. Absent this authority, criminal investigations could be thwarted merely by domestic companies renting server space abroad or using cloud-based services that store data outside the country. In fact, the United States and many other countries routinely exercise domestic authorities to obtain cross-border access to electronic evidence from providers subject to their jurisdiction.

At the same time, even as so many countries reach *out* beyond their borders for evidence vital to their criminal investigations, they also, perhaps instinctively, are wary when other countries reach *in* to their jurisdictions. It is all too easy to see the temptation for national governments, in an effort to protect the safety and privacy of their citizens, to pass "blocking statutes" – restrictions on other countries' access to data controlled within one's own borders. The United States does this as well—our laws impose potential restrictions on disclosure of data by U.S.-based providers that can obstruct efforts by international partners to gain access to evidence controlled by these providers.

It was precisely these kinds of situations that prompted the U.S. Congress to pass the Clarifying Lawful Overseas Use of Data Act – the CLOUD Act. The CLOUD Act is an important step in our efforts to minimize the challenges we all face in obtaining access to electronic evidence stored outside our borders.

The CLOUD Act's Authorization of Bilateral Agreements

What exactly does the CLOUD Act do?

First, it authorized the U.S. to enter into bilateral agreements to facilitate the ability of law enforcement partners overseas to get electronic evidence. American providers generally do not disclose certain electronic data directly to foreign law enforcement authorities for fear of running afoul of U.S. restrictions on disclosure. However, under a CLOUD Act agreement each country removes any legal barriers that may otherwise prohibit compliance with court orders issued by either country. Both countries also agree to allow covered orders to be served directly on providers in the other country, without having to go through the other government or the MLA process. The only law governing the disclosure would be the law of the country issuing the order.

CLOUD Act agreements provide both more access – and more direct access – to the providers holding electronic evidence that is critical in today's investigations. But they do not impose any new affirmative obligation on other countries' providers to comply with U.S. orders, or on U.S. providers to comply with other countries' orders. In addition, these agreements do not impose any obligation on either government to compel companies to comply with orders issued by the other. They simply remove, on both ends, the conflicts of law.

This is a win-win— our law enforcement partners overseas gain a channel to bypass the MLA process. This improves their ability to solve crimes and protect public safety, especially in fast-moving criminal investigations. Under this authority, for example, Korean law enforcement officials could apply for an order from a Korean court, which could then be served directly on Facebook, Amazon, or Google. Meanwhile, for the United States, it eases the pressures on the

overburdened MLA process. Indeed, it seems clear that our overseas partners receive more significant benefits than does the United States from a CLOUD Act agreement. Many major providers are already in the jurisdiction of the United States, and we receive far more requests for electronic data than we send to other countries. Moreover, because fewer U.S. government resources will be needed to process incoming MLAT requests from countries with CLOUD agreements, this should allow the United States to respond to other MLAT requests more expeditiously.

I want to underscore, however, that CLOUD Act agreements are not available to countries that do not respect the rule of law and fundamental human rights. The CLOUD Act does not seek to export U.S. legal standards to other countries, but it does require countries to have a high level of checks and balances in place. In my country, each and every search warrant must pass a demanding probable-cause determination; must be approved by an independent judge; and is subjected to stringent requirements as to scope and established constitutional limits as to jurisdiction. The requirements to intercept real-time content are even stricter. Because U.S. law has some of the highest evidentiary thresholds for investigators to obtain evidence, I suspect that there are few, if any, countries that would qualify if the CLOUD Act had required other countries to adhere to the exact same standards.

Instead, the CLOUD Act is conditioned on foreign partners adhering to certain baseline commitments to privacy and civil liberties. In this sense, the CLOUD Act is privacy- and liberty-enhancing. The Act requires that agreement partners have adequate substantive and procedural laws on cybercrime and electronic evidence on the books. It requires that they ensure that their orders target specific accounts, are adequately justified, and subject to meaningful independent review. It requires that partners confine the use of covered orders to the prevention, detection, and investigation of serious crimes. And such orders cannot infringe on free speech or be used to conduct bulk surveillance. It requires appropriate procedures for handling, retaining, and disseminating data collected by covered orders. And it makes clear that these baseline commitments cannot be bargained away, so they may in some instances need to be accomplished through updates to domestic law. By strictly reserving the benefits of bilateral agreements for liked-minded, rights-respecting countries, the CLOUD Act ensures that efficiencies will not be pursued at the expense of privacy and civil liberties. Rather, it is a solution that allows trusted partners to advance mutual interests based on shared values.

The CLOUD Act's Clarification of Provider Obligations

The entire CLOUD Act agreement framework is premised on the notion that both the United States and its foreign partners will have the authority under their domestic laws to compel production of data held abroad by providers under their jurisdiction. Otherwise, the orders issued under the agreement would not reach such data and the CLOUD Act agreements would be of little practical value to either side. Accordingly, the CLOUD Act also amended an existing U.S. law – the Stored Communications Act – to make explicit the long-held legal principle that a company operating within a country's territory can be compelled to produce stored data within its possession, custody, or control, regardless of where it stores that data.

Far from introducing a new surveillance power, the CLOUD Act codified what had been the longstanding practice in the United States until a single 2016 decision by a court of appeals in a case involving Microsoft. It is well established that a company present in our territory is subject to a order for physical records in its possession, custody, or control, and must produce those records, regardless of where they are stored. For decades, the corollary principle – that a provider in our jurisdiction must produce electronic evidence in its control, regardless of where the provider chooses to store the evidence – has been equally settled. It also ensures that U.S. law complies with long-standing international principles widely accepted throughout the world. Indeed, Article 18(1)(a) of the Budapest Convention requires each party to the Convention to adopt laws under which relevant authorities can compel providers in their territory to disclose electronic data in their possession or control – with no exception for data that a provider controls and chooses to store abroad. The amendment to the Stored Communications Act provided just this – for without it, the United States had fallen out of compliance with its treaty obligations.

Clearing Up Misconceptions

There have been inaccurate assumptions raised about this second piece of the CLOUD Act – that clarified U.S. government authority to compel data held by U.S. service providers overseas. As we have heard it, the concern is that the United States is able to use this part of the CLOUD Act in an unrestrained way to obtain orders requiring U.S. hosting services to disclose the data European governments store in the cloud with such providers.

This false assumption is leading to the adoption of standards in Europe that exclude U.S. companies from government and company cloud storage and require localization, such as EU cybersecurity and data transfer rules currently in development. In large part, these standards are based on an inaccurate perception of how this authority is used.

It is a well-established, fundamental principle that a nation can compel the disclosure of evidence from companies subject to that nation's jurisdiction. Beyond being a requirement of the Budapest Convention, as I discussed earlier, it has also been accepted in Europe. The e-Evidence Regulation that the EU recently reached political agreement on foresees giving that very same power to all EU Member States. The Regulation requires that providers offering their services in the Union be subject to European Production Orders requiring the disclosure of data, regardless of where the providers store the data.

Many countries have comparable powers of compulsion. What matters is not whether the power itself exists, but what safeguards restrict its exercise and prevent abuse. The United States has extremely strong safeguards, foremost among them are those imposed on U.S. government searches by the Fourth Amendment of the U.S. Constitution. The Amendment requires that warrants for content of communications be based on the high evidentiary standard of demonstrating probable cause; that they particularly describe the scope of the search and seizure; and that they be approved by an independent judge. Taken together, these requirements are generally much more stringent than those imposed in other legal systems.

Additional restrictions and safeguards include the following: First, the U.S. Department of Justice's Computer Crime and Intellectual Property Section has publicly advised prosecutors

to seek data from an enterprise, such as a company or government, that stores data with a provider rather than from the provider with which the data are stored, absent special circumstances. This provides important guidance to prosecutors to seek data directly from enterprises, including public sector clients of cloud service providers subject to U.S. jurisdiction. In addition, prosecutors should contact the Department's Office of International Affairs when they become aware they may need evidence located in another country and must obtain approval prior to issuing an order to compel disclosure of such evidence.

The CLOUD Act also does not restrict a provider's ability to challenge the legality of orders requesting data. Indeed, providers are aware of the legal issues involved in hosting sensitive data and have established relationships with U.S. law enforcement to raise questions or concerns about whether orders they receive comply with U.S. legal requirements.

In short, criticisms about this part of the CLOUD Act are inaccurate and short-sighted, not simply because the Act stayed well within international norms, but also because it is critical to ensuring that all governments can fulfill their basic duty to protect the public from those who would do them harm.

Current Status of CLOUD Act Agreements

The U.S.-UK agreement came into effect last fall and has been a game-changer for transatlantic cooperation. The agreement was the result of years of negotiations and required legislative changes by both parties to get to signature. This is in part because of the robust privacy and civil liberties protections required by the CLOUD Act. Our ability to go directly to each other's providers has made important investigations faster and more efficient.

As of July 2023, the UK has sent over seven thousand requests for data under the terms of the agreement to obtain evidence held by U.S providers in a wide range of investigations, from child sexual exploitation to terrorism to drug investigations. For example, in one investigation data sought under the agreement resulted in over two tons of cocaine seized and three suspects arrested. In another high priority sexual exploitation case, data sought under the agreement contributed key information in support of a warrant for the suspect's arrest. Reciprocally, while the United States is issuing far fewer orders under the agreement than the UK, the United States has used U.S. legal process to obtain evidence held by providers in the UK in important U.S. investigations more quickly and easily than we could using the mutual legal assistance channel.

We are quite pleased with how the US-UK Agreement is progressing. It's a good example of how we can make meaningful progress on electronic evidence sharing with partners who are also committed to protecting privacy, human rights, and the free flow of data.

We continue to make progress on CLOUD Act agreements with other countries. After two years of negotiations, the United States and Australia signed a CLOUD Act agreement in December 2021 and we hope to be operational in the coming months. We have also begun negotiations with Canada and the EU, and are in active conversations with a number of other

countries. The initial success that we are seeing with the UK agreement gives me great confidence that we will see similar success with other partners.

As we look to additional foreign partners and new CLOUD Act agreements, it's critical to remember that these partnerships are conditioned on a shared commitment to strong and meaningful safeguards for privacy and civil liberties. Thus, any country interested in a CLOUD Act agreement should consider whether its laws and practices would meet the numerous, stringent safeguards required for the certification, including: adequate substantive and procedural laws on cybercrime and electronic evidence, such as those enumerated in the Budapest Convention; respect for rule of law and principles of nondiscrimination; adherence to international human rights obligations; clear legal mandates on procedures governing the collection, retention, use, and sharing of electronic data; mechanisms for transparency regarding the collection and use of electronic data; and a demonstrated commitment to the free flow of information and a global Internet.

In conclusion, our collective safety and security depend on our ability to obtain lawful and efficient cross-border access to electronic evidence. Cross-border transfers of electronic evidence are necessary and appropriate, and they are a critical component of investigating crime in the 21st century.

The CLOUD Act represents a new way forward. It is a solution that can simultaneously advance the imperatives of public safety and privacy protection in many countries. And it is a cooperative solution – enacted by the United States, but driven by concerns raised by our foreign partners about the status quo – that promises international benefits.

The first CLOUD Act agreement has shown us that this can be a quite successful model for cooperation if countries can satisfy the stringent standards for human rights and due process set forth by our Congress. We look forward to engaging with foreign partners to bring the vision of the CLOUD Act to fruition – a vision that will combat serious crimes more efficiently while demonstrating a shared commitment to core privacy protections for data and individuals.