Written Testimony of Richard Salgado
Principal Member, Salgado Strategies LLC

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

Hearing on "Foreign Influence on American's Data Through the CLOUD Act"

June 5, 2025

Chairman Biggs, Ranking Member McBath, and distinguished Members of the Subcommittee, thank you for inviting me to participate in the hearing this morning and for your leadership on these important issues.

My name is Richard Salgado. I have spent most of my more than 35 years as an attorney working on government surveillance and network security issues like those we are discussing today. This includes serving as the Senior Director for Law Enforcement and Information Security at Google for over 13 years and in a similar function at Yahoo! prior to that. I have also served as a federal prosecutor in the Computer Crime and Intellectual Property Section in the U.S. Department of Justice, and worked in private practice. I've taught and lectured on these issues at law schools. I currently teach about surveillance law at Stanford Law School and Harvard Law School. I also consult with many electronic communications service providers.

It was almost exactly 8 years ago that I testified to the House Judiciary Committee about the need for changes to U.S. law that ultimately were included in the CLOUD Act. I'm honored to be here now that we have gained some initial experience with the Act, and in particular the bilateral agreement with the UK negotiated pursuant to the Act. Even in these relatively early days of its implementation, it is clear that the CLOUD Act provides a promising framework for advancing U.S. national security, supporting public safety, and preserving global trust in American technology. It underscores the importance of finalizing agreements with Canada and the European Union, and beginning negotiations with others.

Recent reports that the U.K. is secretly seeking to compel Apple to globally disable security features in one of its products, in order to expand the U.K.'s surveillance capabilities, are deeply concerning and illustrate the value of the CLOUD Act framework. When a foreign government coerces an American company to weaken, disable, or withhold security protections intended to safeguard users' data worldwide, the impact extends to everyone, including Americans. The harm is immeasurably magnified when such actions occur in secret, through legal proceedings whose existence and outcomes remain unknown even to the U.S. government. More pernicious still would be a foreign government repurposing secrecy to force a provider to deceive users about the compromised

integrity of the service. These actions threaten core U.S. interests in cybersecurity and erode the global competitiveness of American technology providers amidst significant competition from China.

If there is still a reasonable debate to be had over whether the security of products and services offered by American companies should yield to government surveillance, euphemistically called "lawful access" and "going dark," that debate does not belong in secret proceedings, controlled by foreign officials accountable only to their own citizens, in a foreign country, with results that remain unrevealed even to the U.S. government. It belongs in open proceedings, before Congress, conducted by officials duly elected by the American people with the interests of the country at heart.

A fortified CLOUD Act, and additional agreements, offer a pathway forward. With a few surgical changes, the Act can stand as a bulwark against these threats and advance U.S. national interests.

The Origin of the CLOUD Act and Early Signs of Promise

The CLOUD Act was signed into law in 2018 by President Trump. The provisions at issue in this hearing were enacted to address a situation that I described in my previous testimony. The U.S. has laws, often referred to as "blocking statutes," that govern in what situations a U.S. service provider may disclose user data. Before the CLOUD Act, U.S. providers were presumptively prohibited from conducting real-time collection of user data for or disclosing content to foreign governments. There was no exception for foreign legal process even if issued by a jurisdiction that respects the rule of law for an entirely legitimate case. A blocking statute violation can constitute a criminal felony.

Blocking statutes like these are not unusual and many countries have them. Those enacted in the United States carry unique significance, however, due to the remarkable success of U.S. service providers globally. American providers handle an enormous amount of the world's electronic data, which of course can be useful in investigations. The U.S. blocking statutes meant that governments looking to compel American providers to divulge information had to rely on the slow and increasingly bogged down diplomatic mechanisms through the U.S. government, like Mutual Legal Assistance Treaties, or Letters Rogatory. And for some types of evidence collection, those mechanisms were unavailable entirely.

Frustrated at the inability to collect evidence, some countries resort to aggressive, unilateral, punitive measures aimed at U.S. providers. They consider laws to force tech platforms to alter the network architecture to localize data within their borders. Some strong-arm the companies through employee harassment and arrests to pressure companies to turn over user data. Some look for vulnerable spots in network infrastructure to capture communications directly, or require providers to remove security measures. As I noted in my earlier testimony, the situation led to "aggressive investigation efforts that can undermine security in general."

The CLOUD Act was passed to deal with this situation. The idea is that the U.S. will conditionally lift the blocking statutes, on a country-by-country basis, for those that qualify for an executive agreement with the United States. To qualify, a country must satisfy many factors, including demonstrated respect for fundamental human rights, civil liberties, and due process of law. Where a country has such an agreement, the U.S. provider can honor requests for disclosure of user data from that country without fear of running afoul of the statutes.

It is no small matter for the United States to lift these blocking statutes. Blocking statutes can be a legitimate and purposeful exercise of U.S. sovereignty over the conduct of companies under U.S. jurisdiction. Easing the blocks, as the CLOUD Act does, is not necessarily an altruistic concession; it can be a strategic choice that serves national interests. If properly calibrated, the CLOUD Act framework can advance broader U.S. priorities, such as fostering a secure cyber ecosystem that is trusted by governments, financial institutions, and other users, and preserving the global competitiveness of U.S. companies.

With the CLOUD Act now in place, two agreements have been concluded; one with the United Kingdom and another with Australia. The early signs are that CLOUD Act agreements have proven to be valuable, hold great promise for the future, and are worth getting right. The November 2024 report by the Department of Justice submitted to Congress about the implementation of the U.K. agreement reflects that many of the goals of the Act seem to be within reach. Like the Department of Justice report, the transparency reports of various U.S. providers reflect a robust use by the U.K. of the CLOUD Act agreement. We have less insight into the use by Australia of its more recent agreement, which seems not to be fully operational. What we can see from company transparency reports indicates a much lighter usage so far.

The short history we have so far reflects that the CLOUD Act has tremendous potential to facilitate legitimate investigations requiring cross-border electronic evidence collection, resolve conflicts of law, and advance human rights and civil liberties. Realizing that potential depends on the U.S. entering into more agreements. For these reasons, I respectfully suggest that the U.S. complete the agreement under negotiation with Canada and another with the European Union. To fully realize the Act's promise, the U.S. should also consider agreements with a broader range of jurisdictions. Some of these may require more nuanced terms than the two in place now, as Matt Perault and I set out in our vision for the future of the CLOUD Act in a report published by the Center for Strategic and International Studies. (Attached as Exhibit 1).

The Hard Lessons Taught

We have also been reminded, recently and forcefully, that U.S. national interests in cybersecurity, and the global competitiveness of American providers, can be threatened by foreign government efforts to weaken the security of services and products offered by American companies. This lesson comes to us from reports from the *Washington Post* in February that the U.K. is seeking to compel Apple to

disable certain available end-to-end encryption protection on all iPhone backups worldwide. Others in this hearing have ably described the legal proceedings and authorities reportedly relied on by the U.K., so I will not repeat that here.

The reporting raises the possibility that the U.K., eager to capitalize on the U.S. having eased its blocking statutes, is prepared to wield its extraordinary access powers extraterritorially against a major American technology company, one that is a pivotal player in the global communication landscape, and to keep the whole endeavor secret including by preventing the company from telling even U.S. government officials. If the U.K. were to have its way in this scenario, those backups would be available in plain text to U.K. authorities through the CLOUD Act agreement. These backups would also be available to any other government that has a CLOUD Act agreement.

It is true that the CLOUD Act and its agreements prohibit foreign governments from intentionally targeting U.S. Persons, as that term is defined, and individuals in the United States. One should take little solace in these provisions, however. First, they still allow for incidental and inadvertent collection of Americans' data, subject to certain minimization requirements. Second, that data can then be disclosed to the U.S. government in some situations. Third, and probably most important, the deprecation of security leaves all the data, including that of Americans, more vulnerable to malicious insiders and hackers, authorities in the U.S., and accidental exposure. As we are reminded time and again, recently with the Salt Typhoon attack, cybersecurity is an imperative, and the risks of compromise are both real and realized.

Compounding these concerns are recent amendments to the U.K.'s Investigatory Powers Act, often referred to as the "Snooper's Charter." These changes give the U.K. government authority to require companies to provide advance notice of any change that could affect surveillance capabilities. Notification mandates are issued at the sole discretion of the Home Secretary, in secret, without consultation with any others. The Home Office can also gag the subject company from disclosing the notice or its contents. Significantly, the U.K. claims this power extends extraterritorially, including to U.S. companies.

The types of changes that may require prior notice are sweeping. They can include improvements like adding or strengthening encryption, upgrading to more secure equipment or software, or altering the length of time user data is retained. The mandate can go even further, requiring disclosures about future business plans such as discontinuing a service or feature, launching a new offering, or acquiring another company or product.

When paired with other authorities, like that reportedly issued to Apple, these notices could lead to orders from the Home Office prohibiting a provider from implementing changes or carrying through with business plans that were the subject of a notification requirement. This, too, could be done in secret with the company prohibited from telling anyone, including the U.S. government. The U.K. Home Office essentially has a veto power on how American companies innovate and improve

their products, as described in this piece published by *Lawfare*. (Attached as Exhibit 2). Even just a threat that the U.K. might exert this authority over U.S. companies can have a chilling effect on investments in security, forcing U.S. companies to weigh whether contemplated upgrades, architectural improvements or business plans will be met with foreign resistance.

The reported actions of the U.K., and the looming threat that the U.K. will exert its expansive claims of extraterritorial authority over U.S. companies, run counter to the U.S. national interest in preserving a secure and resilient communications and network ecosystem. Ensuring that American providers remain free to deliver secure, trustworthy services worldwide is vital to user trust and data integrity, to the competitiveness of American companies and to the broader strategic goal of maintaining U.S. leadership in secure digital infrastructure.

Recommendations

Regardless of the outcome in the reported secret foreign legal proceeding with Apple, which we may never know, this experience underscores the broader threat of foreign government efforts to covertly weaken the security of products and services offered by American companies. We must now identify and implement solutions. Fortunately, the CLOUD Act provides an ideal framework for this.

There are several ways to address this issue, some I outlined in a piece published by *Lawfare*. (Attached as Exhibit 3). At a minimum, and in the short term, the U.S. government should engage with the U.K., if it has not already, to seek an end to the reported effort against Apple and secure a commitment to refrain from similar actions against other American companies as a condition for continuing the agreement. The agreement itself allows for discussions of this sort.

In the medium to long term, amendments to the CLOUD Act, which will make changes that flow to the agreements and their implementation, are needed.

First, the CLOUD Act should more explicitly address the original goals behind its adoption. There are several ways to accomplish this. These include incorporating, as part of the factors for determining whether a country qualifies for a CLOUD Act agreement, whether that country imposes technical capability obligations, mandates defeating or withholding security features, requires advance change notifications, imposes minimum data collection or retention requirements, or mandates data localization. If during the operation of an agreement the Justice Department learns that a country has adopted any such requirement, the Attorney General should immediately notify relevant committees (including the Senate and House Judiciary committees and the Senate Foreign Relations and House Foreign Affairs committees) and consider action, in consultation with those committees.

Second, the CLOUD Act should declare cybersecurity as a "national interest" that, like free speech, must be respected. To help monitor compliance and identify other potentially harmful actions, the Act could require that the foreign government allow American providers to notify Justice Department officials of surveillance demands and related actions such as assistance or capability requirements. The Attorney General could then notify the relevant congressional committees and consider immediate action, in consultation with those committees.

Third, the CLOUD Act could be changed to give the U.S. government timely information about how the agreements are being used. This could provide the U.S. government with insight into whether demands run counter to U.S. interests, implicate sensitive information or national security concerns, or otherwise affect U.S. policy interests. Under previous diplomatic frameworks, such as the Mutual Legal Assistance Treaty system and other cooperative mechanisms, the U.S. government had at least some visibility into the investigations in which foreign governments were seeking to involve U.S. providers. That layer of oversight is lost when foreign governments issue demands directly to providers under the CLOUD Act, without any obligation to notify or involve the U.S. government.

The EU's e-evidence model might provide inspiration. Under the EU system, if one member state issues a cross-border demand to a service provider based in another member state, it must notify the host country in some situations. That host country then has ten days to review the request and object if it raises significant concerns. A similar mechanism could be incorporated into the CLOUD Act, requiring that any foreign legal demand made to a U.S. provider be simultaneously notified to the U.S. government, potentially with a short window to register objections in defined cases. Such a reform would preserve the CLOUD Act's core efficiency goals while reintroducing an essential layer of national oversight, better aligning the statute with U.S. security and policy interests.

Conclusion

The potential of CLOUD Act agreements to advance U.S. national interests is tremendous. Abandoning this framework in response to the reported action by the U.K. against Apple would be counterproductive. Indeed, part of the solution to this critical issue lies within the CLOUD Act itself. With targeted changes, the Act can serve as a stronger instrument for advancing cybersecurity and preserving the capacity of American companies to provide trusted and secure services worldwide. We should treat this lamentable event as an opportunity to improve the Act. Too much is at stake.

Thank you for the opportunity to discuss these issues.

Written Testimony of Richard Salgado
Principal Member, Salgado Strategies LLC

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

Hearing on "Foreign Influence on American's Data Through the CLOUD Act"

June 5, 2025

Exhibit 1

JUNE 2024

Untapping the Full Potential of CLOUD Act Agreements

By Matt Perault and Richard Salgado

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act **(CLOUD Act),** a law that established a process pursuant to which U.S. tech companies are permitted to disclose user data directly to certain foreign governments in response to their requests to assist investigations into serious matters and which allows companies in other jurisdictions to do the same in response to U.S. requests.[1] The law requires that there be an executive agreement between the United States and the foreign government before doing so, and there are standards the foreign government must meet to qualify for such an agreement.

The CLOUD Act is still in its early stages of being implemented. Since the legislation was enacted into law in 2018, two agreements have been concluded: one with the **United Kingdom** and another with **Australia**. This is certainly progress, but these are relatively easy deals to strike. The really hard work lies ahead, with the European Union in the queue and others in the wings.

CLOUD Act agreements remain a vital and promising tool. Deployed with proper calibration, these government-to-government agreements have the potential to play a valuable role for many agencies worldwide in conducting legitimate investigations while protecting human rights, the rule of law, and the global free flow of information. Used effectively and implemented correctly, CLOUD Act agreements provide an important avenue for law enforcement agencies and have the potential to strengthen other international evidence-collection arrangements.

This policy brief is based in part on the authors' **previous experience** working on government surveillance law and policy at Google and Meta. Working with other industry representatives, academics, and members of civil society, they engaged with the U.S. and UK governments to help shape the core elements of these CLOUD Act provisions.

1 The CLOUD Act is more widely known for also resolving a dispute about whether U.S. law enforcement could use a search warrant to obtain data stored outside of the United States from a U.S. company. That is not the focus here.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

The authors offer three suggestions for better realizing the potential of the CLOUD Act. First, the U.S. government should conclude more agreements with more countries. Second, it should adopt practices to better evaluate the success of the agreements. Third, it should implement mechanisms to better detect and address improper use of the agreements. None of these changes require any alteration of the CLOUD Act itself and can be done by the Department of Justice (DOJ) in partnership with other governments.

A History of Blocking Statutes and the CLOUD Act

THE GROWING SIGNIFICANCE OF BLOCKING STATUTES

For **decades**, evidence and intelligence that a country needs to enforce its laws or protect its national security has sometimes been held by companies in other jurisdictions. Over time, as the services offered by U.S. companies became massively popular around the world, this issue became much more prevalent for foreign jurisdictions than for domestic ones. U.S. law prohibits these U.S. service providers from disclosing certain types of user information unless presented with valid legal process issued by a court in the United States, with some limited exceptions, even when the information pertains to conduct and users entirely outside the country. These are laws not to be trifled with. Violations of these "**blocking statutes**" can constitute criminal felonies.

A blocking statute can advance important public policy goals. A democratic government has a legitimate role in regulating the behavior of companies in its jurisdiction, and Congress would not want a U.S. provider to disclose user data that violates civil liberties. For example, imagine if the Iranian government approached Microsoft with an order to wiretap the Outlook email account of a political dissident who had been organizing a political protest. The U.S. government would certainly not want a U.S. company to assist, and the blocking statute creates a legal barrier to doing so. No doubt Microsoft would not want to disclose the information either, and it could use the blocking statute to explain credibly that it is legally prohibited from doing so.

The United States is not alone in using blocking statutes to advance its values by regulating the behavior of providers in its jurisdiction. In the European Union, Article 48 of the **General Data Protection Regulation** serves to restrict data disclosure to non-EU member governments unless certain criteria are satisfied. France also has a blocking statute **prohibiting the disclosure of information** that would harm French interests. Though with far fewer dramatic consequences (given that most of the big providers are in the United States), these blocking statutes may forbid the providers subject to them from disclosing data directly to U.S. government agencies.

Prior to the CLOUD Act, providers subject to U.S. law were presumptively prohibited from honoring valid legal process for certain types of user information from government agencies outside the United States. This was so even when issued by a rule-of-law respecting government and even when the data was that of the government's own citizens. For example, an email provider operating under U.S. law was not permitted, absent an exception, to comply with a UK order to disclose private email of a user even when the user was in the United Kingdom, the crime to which the messages related was committed in the United Kingdom, and the victim was in the United Kingdom.

Because U.S. blocking statutes were restrictive and inflexible, the countries needing user content information from U.S. providers had to turn to other means. For instance, many countries have **Mutual**

Legal Assistance Treaties (MLATs) or other agreements with the United States, which require U.S. government officials to secure legal process from U.S. courts for foreign investigations.

The first MLAT the United States entered into was with **Switzerland** in 1977. In the 1980s and 1990s, it concluded agreements with countries such as Australia, Canada, Israel, and Jamaica. The pace of MLAT negotiations **accelerated** in the wake of the 9/11 attacks, with the United States eager to use them to aid in terrorism investigations. They worked fairly well before the internet became so prevalent in daily life. This dramatically changed with the rise of U.S. companies providing internet communications services popular with people worldwide. In a matter of years, it was not the United States trying to get MLATs in place to investigate terrorism, but other countries seeking MLATs to secure information from these U.S. providers.

As the popularity of the internet skyrocketed, so did the number of requests made to the U.S. government under these treaties and arrangements. The DOJ's Office of International Affairs, which handles such requests, was **crushed** by the volume. Responses became so delayed that occasionally foreign law enforcement officials could not get the data they needed in time to help with investigations. In 2013, a U.S. **report** estimated that MLAT requests took an average of about 10 months. Countries often did not even bother to invoke MLAT to obtain electronic records.

There are **other diplomatic instruments** to which the United States is a party that also have provisions for mutual legal assistance. These include the **Council of Europe Convention on Cybercrime** (i.e., the Budapest Convention and Second Amended Protocol), the **Inter-American Convention on Mutual Assistance in Criminal Matters**, the Organization for Economic Cooperation and Development **Convention on Combating Bribery of Foreign Public Officials in International Business Transactions**, and several UN conventions covering **corruption**, **organized crime**, **drug trafficking**, and **terrorism**. A foreign government might also ask a U.S. agency to open a joint investigation and share information obtained from U.S. legal process. These diplomatic approaches, loosely speaking, suffer many of the same practical drawbacks as dedicated MLATs.

When foreign governments hit these roadblocks, they did not stop pursuing data. Some jurisdictions responded with aggressive, unilateral, punitive measures aimed at U.S. providers. They considered laws to force tech platforms to **localize data** within their borders, based on the erroneous view that changing the data storage model would expedite law enforcement processing. Most egregiously, they resorted to strong-arming the companies through **employee harassment and arrests** to pressure companies to turn over user data or by **finding vulnerable spots in network infrastructure** to capture communications directly.

Foreign governments pressured not only the tech companies, but also the U.S. government. The DOJ and Federal Bureau of Investigation (FBI) were hounded by countries, including close allies, for a more practical means to secure communications content from U.S. providers. The government, providers, and **civil society** were aligned on the existence of a problem.

Going back to the mid-2000s, many U.S. providers began discussing possible approaches to improve the situation with the U.S. government, including the DOJ and FBI, and with **foreign governments**. Providers' suggestions included increasing the resources available to the U.S. government for MLAT compliance, working with foreign jurisdictions on how to use the MLAT process in a way that reduces

churn arising from malformed requests, and even pushing for a more automated portal through which MLAT requests could be completed (with immediate error checking) and submitted. Some of these recommendations were **implemented**. In addition, some companies also made changes to their own policies and practices to improve response times, such as prioritizing requests that come through diplomatic channels.

All these steps undoubtedly helped reduce some of the pressure on the companies and the MLAT system. None, however, could change the reality that U.S. law was unnecessarily impeding legitimate investigations. For many years, there seemed to be little appetite within the U.S. government to pursue any big changes. With shrugging shoulders, most of the effort was spent trying to get **more funding** for the beleaguered and far-too-manual MLAT system.

WORKING TOWARD A SOLUTION

As conversations matured, a new legal dynamic arose. In a dispute between Microsoft and the U.S. government, **the U.S. Court of Appeals for the Second Circuit** held that search warrants issued under the Stored Communications Act were not valid to compel companies to produce data that was exclusively stored outside the United States. The Supreme Court agreed to hear the case, which was then **fully briefed** and **argued**. In the view of the U.S. government, a Supreme Court ruling upholding the Second Circuit's would have hamstrung U.S. law enforcement agencies in pursuing data stored overseas.

Keen to avoid such a ruling, the DOJ saw an opportunity to pursue a bill that would **ultimately moot** the pending Supreme Court case and, more importantly for the purpose of this article, give some hope to other countries that they would have an easier path to securing information from U.S. providers. **Some** members of Congress also reenergized legislative proposals such as 2015's **Law Enforcement Access to Data Stored Abroad Act** and the iterative **International Communications Privacy Act**.

Ultimately, the companies and the DOJ focused on one important observation: Often the U.S. government has no interest in preventing a U.S. provider from honoring foreign legal demands. If Japan needs to obtain emails in a Gmail account sent between two citizens of Japan suspected of committing a murder that took place in Japan, then why should U.S. law stand in the way? It is hard to identify any public policy interest of the U.S. government that would be served in preventing that investigation from progressing.

From this was borne an Obama administration **proposal** to Congress that would ultimately become the **CLOUD Act**. Put simply, the United States would lower its blocking statutes under the conditions set out in the legislation and pursuant to an executive agreement for any country that meets certain minimum standards on human rights and the rule of law. This would allow, but not require, U.S. companies to honor the foreign legal process from such countries. One condition, among many, was that the other government would do the same with regard to its own blocking statutes.

Hearings were had, **blog posts written, debates held**. Many civil society groups were **decidedly skeptical**. Ultimately, and to the surprise of many, the CLOUD Act (including the provisions allowing for the lowering of blocking statutes) found its way into a must-pass **appropriations bill**, and President Trump signed the CLOUD Act into law on March 23, 2018.

CLOUD ACT AGREEMENTS REALIZED

Even before the CLOUD Act became law, the U.S. government had its eye on inking a deal with the United Kingdom. **Conversations** between the DOJ and Home Office officials likely informed what was included in the final bill. But even with this head start and a very eager ally on the other side of the table, it takes time to negotiate and implement a law enforcement agreement.

First, the CLOUD Act agreement is a novel type of arrangement, requiring the countries to develop bespoke terms. Previous diplomatic accords such as MLATs might have a few clauses that are transferable to CLOUD Act agreements, but they differ in significant ways and do not provide easy templates.

Second, even though the United States and the United Kingdom have relatively similar legal systems, the United States understood that this agreement would likely serve as a starting point for agreements with other jurisdictions where there are much greater differences. The agreement with the United Kingdom had to take into account potential sticking points or tensions arising in negotiations with other countries.

Third, each side had to be careful to protect what is referred to in diplomat-speak as "essential interests." The United States wanted to make sure that information provided by U.S. providers under the agreement would not be used in a manner that raises free speech concerns. The United Kingdom considered the potential impacts of direct disclosures from UK providers in U.S. death penalty cases. Both insisted that before prosecutors can use information collected from its providers as evidence in a case that implicates the respective essential interest, the prosecutors must secure permission from the other's government.

In spite of the inherent headwinds, the U.S. government concluded the negotiations with the **United Kingdom** in October 2019 and those with **Australia** in December 2021. At least two other agreements are currently being negotiated: one with **Canada** and one with the **European Union**.[2]

Because they have CLOUD Act agreements in place, Australia and the United Kingdom now have more options for pursuing data they need to assist with important investigations. Providers now have fewer restrictions for responding to these requests and greater clarity on how the data will be treated following a disclosure. The U.S. government presumably has fewer diplomatic requests from these countries than it would have otherwise. And because of this reduction in requests from countries with agreements in place, other jurisdictions may be experiencing a relatively faster response to their requests for assistance from the U.S. government using traditional diplomatic means. This is a good start, but there is plenty of room for more.

Releasing the Potential of CLOUD Act Agreements

This brief offers three suggestions that can help the CLOUD Act reach its full potential. First, the U.S. government should work to conclude more agreements with more countries, avoiding the

2 The EU negotiations are very complex, presenting far more issues than the bilateral arrangements with the United Kingdom and Australia. For political optics, some future agreements, including perhaps the EU-U.S. arrangement, will likely not be overtly referred to as "CLOUD Act Agreements" and may cover other issues while still invoking the CLOUD Act provisions. This is in part because the CLOUD Act is known less for conditional lifting of U.S. blocking statutes and more for the provision that allows the United States to compel a U.S. provider to disclose data in its possession, custody, or control regardless of where the data is located (subject to other objections). These two provisions are at times conflated, the latter rightly or wrongly tainting the former. Avoiding the CLOUD Act brand altogether, as the European Commission has done, may help avoid confusion.

perception that the CLOUD Act is designed to create a "club" of countries with preferred data access. It can expand participation by using a series of "knobs and levers" to tailor agreements to specific jurisdictions. Second, it should adopt practices to better evaluate the agreements, including increasing transparency. Third, it should implement mechanisms to better detect and address improper use of the agreements.

A BIG TENT, NOT A PRIVATE CLUB

Carefully crafted CLOUD Act agreements can play a positive role for many countries beyond those in the Five Eyes (consisting of Australia, Canada, New Zealand, the United Kingdom, and the United States) and the European Union. At times, the DOJ has made it harder to realize a "big tent" vision for the CLOUD Act by describing it in terms that suggest a "club" mentality. When the DOJ says that CLOUD Act agreements are only available to "trusted foreign partners," it is telling all the others, even those that can meet the standards, that they have to find their own way.

There will be a concrete negative effect if there is a perception that the CLOUD Act creates a fast lane only for countries that have gained admission into a privileged club. If countries such as India and Brazil feel like outsiders, they are more likely to respond with measures the CLOUD Act **aims to avoid, including** data localization, fines, arrests, and other retributive policies.

To conclude more agreements with more countries, the U.S. government should (1) explore a broader range of agreement terms; (2) avoid suggesting that CLOUD Act agreements are only for a "club" of favored nations; and (3) devote more dedicated resources to negotiating CLOUD Act agreements.

The first step in concluding more agreements is broadening what an agreement might look like. The CLOUD Act agreements with the United Kingdom and Australia are very similar, with both nearly as expansive as the statute allows. They both apply to the broadest array of crimes permitted by the statute, can be used by a wide range of agencies in each country, apply to collecting data in a stored state as well as real-time surveillance of communications, allow targeting to the maximum extent permitted by the statute, and are subject to congressional review only within the shortest permissible time frame.

Based on these two agreements, one might mistakenly assume that all CLOUD Act agreements must look this way. The CLOUD Act itself, however, does not require that every agreement extend as far as the law permits. In fact, as expansive as the agreements with the United Kingdom and Australia are, both amend the baseline requirements of the CLOUD Act to impose restrictions on using data disclosed to U.S. authorities as evidence that could lead to the imposition of the death penalty. Just as the United Kingdom and Australia could insist on terms that make the agreements stop short of the full extent allowed by the statute, the United States can do the same in future agreements.

There are many levers and knobs that can be adjusted to accommodate for differences in legal systems and particular needs and sensitivities:

- **Covered Crimes:** Agreements could apply only to specified serious crimes, with shared definitions across borders, such as investigations into acts of terrorism or cybercrimes.

- **Participant Agencies**: Agreements could apply only to particular investigative agencies. For example, the blocking statutes in the United States might be lowered under an agreement only for requests from an agency that has a track record for high quality investigations and is subject to meaningful oversight.
- **Surveillance Type:** Agreements could limit the nature of data acquisition. For example, an agreement could allow for collection of stored content but leave intact the U.S. blocking provisions for real-time surveillance.
- **Surveillance Duration Limits:** Similarly, agreements could restrict the surveillance period. For example, stored communications could be limited to a 6-month period and real-time surveillance to 60 days.
- **Targets:** Agreements could limit which users may be targeted in the requests. Although the **CLOUD Act** prohibits the non-U.S. country from intentionally targeting a U.S. person, an agreement could impose additional restrictions. For instance, it could limit the targeted users to only those who are reasonably believed to be located in or citizens of the requesting country, as well as in jurisdictions that have not agreed to certain international standards (such as the Second Additional Protocol to the Budapest Convention).[3]
- **Government Insight on Disputes:** Agreements could expressly allow a provider to object to a request by notifying its home jurisdiction of the issue at the same time as it submits its objection to the requesting government. The authors describe this type of dispute management below.
- **Government Insights on Overall Use:** For even more timely visibility into the requests made to providers, agreements could include a requirement that when an agency submits a CLOUD Act demand to a U.S. company, it must also send a copy of the demand to the DOJ.
- **Compressed Review Periods:** Agreements could require shorter terms, triggering more frequent reviews of the country's qualified status for renewal. The authors describe additional oversight options in more detail below.

Moving away from a one-size-fits-all approach will expand the range of countries that could negotiate and secure a CLOUD Act agreement. Many agreements might be narrower than the ones in place with the United Kingdom and Australia, which might mean that the pool of potential CLOUD Act agreement countries **would not be limited** to those with legal systems similar to that of the United States. This will give a wider range of governments optimism that they can conclude such agreements and in turn incentivize them to develop options for improving their laws.

> *Moving away from a one-size-fits-all approach will expand the range of countries that could negotiate and secure a CLOUD Act agreement.*

3 Experience with the current CLOUD Act agreements will be instructive on this point. The scenarios painted for Congress to show how the UK agreement could be used by the United Kingdom often had the targeted user in the United Kingdom, but neither the legislation nor the agreement limits targeting in this way. Government reports, if released to the public, will likely reveal that most of the targeted users are outside the United Kingdom.

Obvious candidates for fine-tuned CLOUD Act agreements include India and Brazil. Both have historically issued a large number of demands on U.S. providers. The frustration their respective law enforcement and intelligence services have experienced with existing disclosure mechanisms has led to a slew of proposals that could be detrimental to security and privacy. Another candidate for an agreement is South Korea, which has had a **dramatic** increase in **requests** for user information from U.S. providers in the last few years,[4] and which the DOJ has **referred to in its hypothetical CLOUD Act scenarios**.

Scholars such as Peter Swire, Deven Desai, and DeBrae Kennedy-Mayo **have shown** that **India presents** an important candidate for improved data disclosure. India, like many jurisdictions, has laws and practices that may require significant changes to meet the minimum requirements of the CLOUD Act. As Swire and Kennedy-Mayo postulate, these might include India joining the Budapest Convention, forswearing the use of legal process that does not involve a judicial authority, and using a "qualified entity" to act as a moderator on behalf of requesting agencies to enforce policy requirements regarding requests to providers. On the other hand, excluding India entirely could invite more aggressive and counterproductive unilateral action, which is likely to have a negative impact on the privacy and security of people in India and beyond. Figuring out a path for a more limited agreement would reduce the likelihood that the government takes such steps and could create an incentive for it to institute domestic reforms in hopes of securing a more expansive agreement in the future.

This presents the DOJ with a very challenging objective: to aim for a "big tent" approach while also protecting U.S. interests in situations that justify interference through blocking statutes. Regulating the behavior of a U.S. company makes sense when the requesting country is corrupt and contemptuous of the rule of law or commits human rights abuses. And of course, the United States has an interest in protecting U.S. individuals who may be the subject of a request from a foreign government to a U.S. provider.

For these reasons, U.S. government officials should be clear that foreign governments must meet certain standards to participate. Of course, it is also possible that countries such as India and Brazil may balk at the prospect of entering into agreements that are more limited than others have been in the past. Hopefully, the immediate value of even a narrow arrangement and the potential for future expansion will overcome the tendency toward such a reaction.

Finally, to accelerate the pace of negotiations and conclude more agreements, the DOJ needs resources. Congress should allocate increased funding for this program, including adding personnel dedicated to negotiating CLOUD Act agreements with a greater set of countries. Devoting resources to the CLOUD Act process so it can respond to more requests would also free up resources for and complement other data access mechanisms such as MLAT and letters rogatory.

In addition, an agreement with the European Union, currently under negotiation, presents a good example of how the CLOUD Act can fill gaps left by other mechanisms. Even after EU member states have adopted the new **E-Evidence Directive and Regulation** so they can obtain data from the EU subsidiaries of U.S. providers established in Europe (often in **Ireland**), these countries' law

4 See, e.g., Google Transparency Report (reporting 774 requests covering 2,788 accounts in the first half of 2019, rising to 2,747 demands covering 16,609 accounts in the same period in 2023); Facebook Transparency Report (reporting 351 requests covering 1,932 accounts in the first half of 2019, rising to 1,468 requests covering 1,932 accounts in that period 2023).

enforcement agencies will still need to use diplomatic mechanisms to obtain evidence about users served by the providers' U.S. entities. For agencies in EU member states, an arrangement that takes advantage of lowered U.S. blocking statutes through the CLOUD Act could be valuable to their legitimate investigations into threats involving non-U.S. users of the U.S. providers.

CLOUD Act agreements also complement the Budapest Convention. Being a party to this convention is specifically called out in the CLOUD Act as a factor to qualify for an agreement. As a result, the desire for such agreements may incentivize more countries to sign on to it, including the Second Additional Protocol. This would be a valuable end in itself, and **even more so** by incentivizing countries away from other international instruments lacking in basic protections, such as the draft **cybercrime treaty** before the United Nations.

EVALUATING EFFICACY

It is important to be able to identify whether a CLOUD Act agreement is effective in removing unnecessary barriers to legitimate investigations and improving, or at least forestalling backslide, on human rights. Understanding impact will help the United States develop options to improve agreements or perhaps will suggest that investment should be made in other mechanisms. It will also enable nongovernmental organizations (NGOs) and academic researchers to evaluate the CLOUD Act process. Finally, since Congress receives reports on the operation of each agreement, understanding impact will be critical for that review process.

The DOJ posts information about related negotiations, agreements, and public communications on its **CLOUD Act Resources webpage**, but there is no data about the volume or type of data requests. While the UK government has provided **some information**, it has not yet provided much detail.

During CLOUD Act negotiations, the United States and companies discussed options for ensuring that there would be transparency about how the agreements worked in practice and accountability for violations. But in practice, transparency and accountability are difficult. Not only does it take time to collect and report data, but the agreements are still in their early stages. The first agreement, with the United Kingdom, came into force **on October 3, 2022**, and data requests did not immediately ensue. In addition, collecting information about how an agreement is used is challenging because of how the current CLOUD Act agreements work. If the United Kingdom uses the CLOUD Act to request data from a U.S. provider, the DOJ might never see that the request was made unless the provider raises a dispute with the United Kingdom that is not resolved, so the U.S. government gets pulled in. Removing the provider's host government from this process, in cases where the host government does not have an interest in the request, is precisely the point.

As understandable as the challenges of transparency might be, the lack of it makes it difficult to understand the efficacy of CLOUD Act agreements. This means the DOJ and Congress would face challenges in making this assessment, as would third-party organizations and experts such as NGOs and academic researchers.

To improve transparency, CLOUD Act agreement participants should make available qualitative and quantitative information about how the agreements function in practice. The agreements in place with the United Kingdom and Australia each allow agencies in those countries to submit requests directly to U.S. companies with no notice to the DOJ. Yet there is nothing in the legislation prohibiting

agreements from including a requirement that when an agency submits a CLOUD Act demand to a U.S. company, it must also send a copy to the DOJ. More detailed and timely information could help the department catch issues sooner and provide better analysis to Congress when an agreement comes up for review. This requirement should be reciprocal, necessitating that the United States also copy the central authority of the other government when it issues a request under the agreement. Of course, it is important that the DOJ not use this notification as a preapproval process for every request submitted by the host country; that would reintroduce the very pitfalls of the MLAT system.

Currently, the agreements require each government to submit annual reports providing "aggregate data" on its use of the agreement. The first such reports from the United States and the United Kingdom should have already been generated and exchanged, but so far they have not been made public. Perhaps, given that the first anniversary of the agreement with the UK going into effect was recent, the reports are still being reviewed. Regardless, the DOJ should make these reports public, including its own. The CLOUD Act does not require that the reports be kept confidential, nor do the agreements now in place. If there are good reasons not to publish them in full, the DOJ should consider releasing summaries with qualitative and quantitative data on how the agreements are working in practice. In any event, these full reports should be made available to Congress. Similarly, the CLOUD Act requires that when an agreement is up for renewal, the DOJ submits a report to congressional committees setting out how the agreement has been implemented and describing any problems or controversies encountered. As with the annual reports, the DOJ should make these publicly available to the extent it can.

In addition, companies should publish data in their transparency reports on the number of CLOUD Act requests they receive and by which country, as **Meta** and **Google** have already done, for example. (The agreements currently in place require that demands indicate they are issued pursuant to the agreement, making it relatively easy for providers to track.) But company reporting is likely to create a spotty and incomplete picture of the total impact of the CLOUD Act. The key information is the total number and type of requests from foreign governments, not the requests that each provider received.

Governments should not be the only entities reviewing the efficacy of the agreements. With funding from foundations and governments, civil society organizations should also study their impact, including their long-run influence on human rights norms. For instance, Freedom House, a nonprofit organization, releases an **annual report** on internet freedom. With dedicated support, it could expand this report to include detailed analysis of the CLOUD Act's annual impact. Freedom House or other think tanks might serve as a repository for company reporting, providing a more holistic overview of requests made pursuant to the agreements.

ENFORCING AGAINST VIOLATORS

The robust process required by the statute to qualify for an agreement under the CLOUD Act is essential to its purpose. As the United States looks at other jurisdictions with which to enter more bespoke arrangements, it may need to adopt additional protections against misapplication of the agreement. It is also possible that a country might change its legal authorities after entering into an agreement, and those changes might warrant revisiting its "qualified status." This means the United States will need

a mechanism to detect whether the agreement is being misused or the law has changed and to take action in response.

One obvious way to gain such insight is by setting up a process for a U.S. company to immediately report objectionable CLOUD Act agreement requests to the DOJ. The agreements with the United Kingdom and Australia each allow a provider to raise initial objections with the issuing authority. If the objection is not resolved, the provider may bring in its host government so that the two governments can hash it out. Significantly, the agreements currently in place do not prohibit a provider from notifying its host government at the same time as it submits the objection to the requesting government. There is no process for doing so, however. To gain more visibility into the nature and volume of requests that are out of the agreements' scope or otherwise problematic, future agreements could make this explicitly permissible and set up an intake process with the DOJ.

Once it has more timely insights into the disputes arising with U.S. providers, the DOJ could take action if it believes the foreign government is violating the terms of the agreement or decide to refrain from interfering and let the objection process in the foreign jurisdiction play out. If the DOJ does see systemic issues, it could apply pressure on the other country, noting that its qualifying status may be in peril. In addition, regardless of whether it takes action in individual cases, it could inform Congress of these objections during the review period. The DOJ could strengthen its hand in these circumstances by including a provision in each agreement that allows it to immediately suspend it on the grounds of misuse.[5]

Another accountability mechanism would be to build in more frequent opportunities to revisit the terms. The CLOUD Act provides that any agreement will expire after five years but may be renewed if the U.S. attorney general and secretary of state provide a report to Congress concluding that the other country is still "qualified." Individual agreements could have shorter terms and require more frequent reviews. In addition, an agreement could expressly provide that it is subject to an immediate pause, suspending further submission of requests, if there is a need to address sudden material changes in circumstances. Armed with more information from periodic public reports, more frequent reviews might also incentivize faster improvements in the partner country since they could lead to a more expansive arrangement in a shorter time.

> *The United States will need a mechanism to detect whether the agreement is being misused or the law has changed and to take action in response.*

Conclusion

CLOUD Act agreements have tremendous potential, alongside other diplomatic mechanisms, to facilitate legitimate investigations that require cross-border electronic evidence collection without

5 The agreements with the United Kingdom and Australia have similar provisions to preclude use of the agreement for an identified category of requests when a dispute is not resolved and to allow the agreement to be terminated with one month's notice.

sacrificing human rights and liberties. To get closer to that potential, a series of knobs and levers should help guide future negotiations, since a one-size-fits-all approach would unnecessarily constrain the CLOUD Act's reach. The United States should also build in more mechanisms for transparency and accountability to help identify areas of improvement, ferret out otherwise hidden problems, and build trust. ■

Matt Perault *is the director of the Center on Technology Policy at UNC-Chapel Hill, a professor of the practice at UNC's School of Information and Library Science, and a consultant on technology policy issues at Open Water Strategies.* ***Richard Salgado*** *is a senior associate with the Center for Strategic and International Studies' Strategic Technologies Program, teaches at Stanford Law School and Harvard Law School, and provides consultancy services through Salgado Strategies LLC.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

Written Testimony of Richard Salgado
Principal Member, Salgado Strategies LLC

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

Hearing on "Foreign Influence on American's Data Through the CLOUD Act"

June 5, 2025

Exhibit 2

LAWFARE

Cybersecurity & Tech Surveillance & Privacy

Surveillance-by-Design in Proposed Amendments to the U.K. Investigatory Powers Act

Jim Baker, Richard Salgado

Friday, January 19, 2024, 4:00 AM

The U.K. government is considering making significant changes to its primary government surveillance authority, the Investigatory Powers Act. Some of those changes are ill advised and will negatively impact the security of its citizens.

There is a bill moving rapidly through the U.K. Parliament that poses a significant threat to data security and privacy in the U.K. and beyond. It is ill considered and should be amended substantially before it moves forward.

The bill is flawed in several respects, as some observers have pointed out. This piece focuses on certain elements that we think will stifle innovation and substantially hinder the efforts of private companies to enhance, or even maintain, core security and privacy products, features, and architecture, especially with respect to the use of encryption. To be sure, governments in democratic countries face challenges in accessing the content of communications of spies, terrorists, and other threat actors. They need help. But these purported solutions in the bill aren't the right way to do it.

Specifically, the proposed amendments to the 2016 Investigatory Powers Act would give the U.K. government, at the sole discretion of the secretary of state for the Home Department (Home Office), the power to require a company to tell the U.K. government about new or changed products or features before the company could launch them. This mandate could be issued without consultation with privacy regulators or others in a position to opine on proportionality or other considerations, much less a judicial review.

Following receipt of a "Notification Notice" (yes, that's actually what it is called), the U.K. government could use existing powers to require that the company meet surveillance capability demands as a condition of making a product or feature available. Demands are left to the discretion of the government and could include, for example, disabling security like encryption, user access controls, and privacy protection features. If the government's demands are not met, the company may have no choice but to abandon the product or feature launch, giving the government essentially a veto power on how companies innovate and improve their products. (The government could even block a company from deprecating a service or deleting data.) All of this is done secretly, with the company prohibited from disclosing it unless the government allows it to do so. The act purports to extend enforceability to non-U.K. companies, and the amendments expand that to retention and these notices, exacerbating the challenges that companies face. Paired with the gag order that comes with each, this has several effects, including that the non-U.K. company can't notify its home government of the demand, even one that violates the law of the home government, preventing any sort of diplomatic assistance.

The Home Office has been very explicit that the purpose of the amendments is to "ensure continuity of lawful access to data against a background of changing technology." It's understandable that the U.K. intelligence and law enforcement agencies would like to know about a company's research and business plans, and have a say in whether and how a company makes a change that has serious implications for their weighty missions. Both of us have worked in law enforcement, and we know how important, and how difficult, the jobs of public safety officials are. There's no reason to think that the intentions behind the bill are anything but noble. This proposed power, however, goes too far and is counterproductive.

First, there's no case that this extraordinary power would solve any existing problem. Most providers are quite transparent about product launches, feature additions, and removals. Many companies have entire conferences to loudly trumpet what is coming, or at least issue announcements through blog posts and press releases. In addition, there's no shortage of dialogue between the U.K. government and technology providers. In October 2023, U.K. security officials and their Five Eyes partners (the United States, Canada, Australia, and New Zealand) made a high-level and highly publicized visit to meet with technology companies in Palo Alto, California, to discuss a range of security topics, including espionage

threats from China. On top of there being no clear problem to solve, the amendments could chill companies from engaging with the government in this otherwise healthy exchange about technological innovations for fear of enticing the government to issue a notification notice. The open cooperative dynamic is at risk of being replaced by one that is defensive and adversarial.

Second, this new product approval regime could harm British users and other users around the world. A company that ultimately must capitulate to the surveillance demands of the government may end up offering services that are less secure generally, susceptible to compromise by bad actors, state sponsored or otherwise. Perhaps as a result, the U.K. will have its narrow surveillance needs met at a particular moment in time, but this would come at a great cost to those users specifically, and cybersecurity generally. One of us has testified to Congress and one written at length about the importance, for example, of encryption in enhancing cybersecurity for society, while also working to find a more effective path forward for everyone. This bill, if enacted, could easily be used to stifle the increased use of encryption to protect data security and privacy.

Third, enacting this bill will seemingly legitimize this heavy-handed approach for countries less steeped in the rule of law and with a lower regard for human rights. Should the current version of the amendments pass, even if U.K. authorities adhere in exemplary fashion to human rights and privacy concerns, other security services, especially in authoritarian-leaning countries, will not. They could endeavor to replicate the U.K.'s secretive power in order to undermine product security for their own aims, not only to surveil users but also to censor their communications. No country should expect it will necessarily be the beneficiary of the use of this new power to control and direct product development. It's purportedly designed for use by the U.K. and for the U.K., though resulting insecurities will be there for any actor to exploit if they can find them.

The proposal also runs counter to other efforts by numerous governments—including the U.K.—to urge the private sector to find better ways to substantially enhance cybersecurity on a more sustainable basis. Instead of doing that, the bill, as currently drafted, jeopardizes data security and privacy in pursuit of an understandable goal of helping law enforcement and intelligence agencies' legitimate objectives. But no one needs a law that could limit future progress on much-needed security enhancements, such as through the increased use of encryption. The bill needs to be fixed.

Jim Baker

𝕏 @thejimbaker

Read More

Jim Baker is a contributing editor to Lawfare. He is a former Deputy General Counsel of Twitter, the former General Counsel of the FBI, and the former Counsel for Intelligence Policy at the U.S. Department of Justice. In that latter role, from 2001-2007, he was responsible for all matters presented to the U.S. Foreign Intelligence Surveillance Court. The views expressed do not necessarily reflect those of any current or former employer.

Richard Salgado

Read More

Richard Salgado teaches at Stanford and Harvard Law Schools. He also serves as an Advisory Board Member of American University Washington College of Law's Tech Law and Security Program, a Visiting Fellow on Security and Surveillance with the Cross-Border Data Forum, and a Senior Associate (Non-resident) with the Center for Strategic and International Studies. Richard founded a consultancy to provide guidance to organizations navigating cybersecurity and surveillance challenges. Richard has over 35 years of experience across the private sector, government and academia, including as Google's Director of Law Enforcement & Information Security for 13 years, and as a prosecutor with the Computer Crime and Intellectual Property Section of the Justice Department.

Written Testimony of Richard Salgado
Principal Member, Salgado Strategies LLC

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

Hearing on "Foreign Influence on American's Data Through the CLOUD Act"

June 5, 2025

Exhibit 3

LAWFARE

Congress Cybersecurity & Tech Surveillance & Privacy

First Insights Into the U.S.-U.K. CLOUD Act Agreement

Richard Salgado

Monday, March 10, 2025, 8:00 AM

A Justice Department report reflects early success and shortcomings of the agreement, especially around protecting U.S. cybersecurity.

The Department of Justice recently renewed its CLOUD Act agreement with the United Kingdom. It also submitted a report to Congress, the first of its kind, offering an initial glimpse into the implementation of the agreement. The report reflects some early success, unexpected shortcomings, and several significant issues that policymakers must address.

The report has far fewer details than Matt Perault and I have previously called for, but it does appear anecdotally that the U.K. has found the agreement valuable, as has the U.S., but to a vanishingly small extent. At the same time, the agreement falls significantly short of meeting essential goals. The report suggests, in muted tones, that the U.K. bears responsibility for these shortcomings and can rectify them. When read in light of the recent reports that the U.K. is aggressively pursuing Apple in another attack against encryption, it also highlights the untapped potential that remains with these agreements, and how all of them must be fortified if they are to achieve the noble aims of the CLOUD Act and protect national interests.

A Primer on the CLOUD Act Agreement

Due to the popularity of the services they offer around the world, U.S. service providers hold an enormous amount of user data, data that is subject to U.S. law, including important privacy provisions. Foreign jurisdictions conducting criminal

investigations increasingly found that evidence they needed was in the hands of these providers, and getting it was no easy task due to U.S. law blocking disclosures.

These investigators typically needed to rely on a slow diplomatic process, like mutual legal assistance treaties (MLATs) that required the U.S. government to get the information from the U.S. providers through the courts. This was true even in investigations in which the U.S. had no need to be involved. The U.S. MLAT process became even slower as an onslaught of requests came in from around the globe. (To a far lesser extent, criminal investigators in the U.S. faced similar problems seeking information from providers abroad.)

This issue led jurisdictions to consider or pass unilateral extraterritorial surveillance laws meant to reach across shores to U.S. companies and force them to disclose user data without regard to U.S. law or equities the U.S. has in when U.S. companies disclose user data. Some of these surveillance laws also imposed requirements that the companies have surveillance capabilities or localize data, or take other steps to defeat security features to the detriment of cybersecurity and privacy.

The CLOUD Act agreement provision was intended by Congress to advance the following goals:

- Allow foreign countries to more effectively investigate legitimate cases of serious crime while protecting human rights, the rule of law, and essential interests of the U.S.
- Reduce the burden on the Justice Department and U.S. courts by allowing U.S. providers to disclose data directly to jurisdictions with which the U.S. has an agreement, avoiding government-to-government mutual legal assistance processes. (Although not a primary one, another goal was to allow providers in the other jurisdiction to disclose data to U.S. authorities on the same terms.)
- Reduce the incentive foreign countries have to impose surveillance-related laws on U.S. companies.

To achieve these goals, the CLOUD Act changed U.S. privacy law to allow U.S. companies to disclose user data in response to legal requests from foreign jurisdictions subject to conditions, including:

- There must be an executive agreement in place between the U.S. and the other country, and to qualify for an agreement, the other country has to meet human rights standards and honor the rule of law, among other requirements.
- The demands to U.S. providers must "be for the purpose of obtaining information relating to the prevention, detection, investigation, or prosecution of serious crime, including terrorism."
- The information demanded may not be that of someone physically in the U.S. or an American citizen, national, or permanent legal resident.
- The demands may not interfere with essential national interests, including freedom of speech.

Of course the arrangement was reciprocal, so the providers in the other jurisdiction should be able to honor similar requests from U.S. law enforcement. Given that so much of the world's information is held by U.S. providers, it is understood that the U.S. is unlikely to use CLOUD Act agreements as much as the other parties.

The first agreement, with the U.K., went into force on Oct. 3, 2022. The only other country to enter into a CLOUD Act agreement thus far is Australia. By law, each expires after five years unless renewed.

The First CLOUD Act Report to Congress

The Department of Justice recently renewed the agreement with the U.K., as the report reflects. As part of that, it submitted a report to Congress as is required by statute. There are five key insights from the report that policymakers should consider.

1. The U.K. has availed itself of the agreement with vigor and almost entirely for intelligence gathering through wiretapping. As of October 2024, the U.K. issued 20,142 requests to U.S. service providers under the agreement. Over 99.8 percent of those (20,105) were issued under the Investigatory Powers Act, and were for the most part wiretap orders, and fewer than 0.2 percent were overseas production orders for stored communications data (37). The Justice Department characterizes this as "robust" use of the agreement. Google has begun reporting statistics on its receipt of CLOUD Act requests, and they are largely consistent with the numbers in the report.

2. The report provides no information on what percentage of the 20,142 requests revealed any useful information, but does present some context-free illustrations that demonstrate the usefulness of information obtained through the agreement.

Relying on representations from the U.K., the report reflects that in the first half of 2024, the agreement "contributed directly to 368 arrests, the seizure of 3.5 tons of illicit drugs, the recovery of GBP 5 million, the seizure of 94 firearms and 745 rounds of ammunition, and the identification of 41 threats to life and 100 threats of harm."

3. The U.K.'s implementation of the agreement has failed to advance Congress's intended goal of alleviating the burden on the Justice Department and U.S. courts.

The CLOUD Act agreement provision establishes an alternative channel for foreign law enforcement agencies to obtain information from U.S. providers, bypassing traditional and infamously slow diplomatic routes such as MLATs. Nearly all of the requests made by the U.K. through the agreement, however, could never have been made using diplomatic procedures, since MLATs cannot be used for wiretapping authority, so they displaced none of that burden. On top of that, the U.K. has continued to use the MLAT process at the same rate as before the CLOUD Act.

4. The U.S. has used the agreement very little (as expected), with mixed results.

The United States made 63 requests to U.K. providers between Oct. 3, 2022, and Oct. 15, 2024. All but one request was for stored information. The Justice Department report says that information obtained from U.K. providers helped "further investigations against computer intrusion, fraud, money laundering, threats and extortion, tax offenses, and customs violations, among other criminal activity."

The low volume relative to requests from U.K. authorities to U.S. providers is expected for a few reasons. First, as the report acknowledges, unlike the U.S., the U.K. does not have many service providers with a user base that spans the globe. Most of the providers offer services only within the country. The agreement does not allow the U.S. to submit requests to those providers for information about U.K. persons, so most of the users are off limits. Second, most of the providers in the U.K. are phone companies, not email, social media, or cloud providers. Thus, the scope of information is limited. Third, related to the first two reasons, the U.K. providers have relatively fewer users overall.

One irony to note is that, as lightly as the U.S. is using the agreement, it's likely that the agreement has decreased the burden on the U.K. MLAT system in processing U.S. requests more than it has on that of the U.S. MLAT system in processing U.K. requests. Here's why: 62 of the requests made by the U.S. would have otherwise gone to the U.K. through the MLAT system (assuming the U.S. cared enough to invoke the MLAT process for the data). At most, only 37 of the U.K. requests under the agreement might have qualified for the MLAT process.

Something unexpected that the report revealed was the Justice Department's various challenges in its engagements with U.K. providers. The report detailed the reluctance of some U.K. providers to cooperate with U.S. requests. This hesitancy, according to the Justice Department, comes from "lingering data protection concerns" about possible liability under U.K. law if they were to disclose data. The Justice Department also politely complains that the U.K. government has done little to make sure U.K. providers know that they are permitted to honor U.S. requests. According to the report, the U.K. government is looking to amend the data protection law to remove any doubt about the legality of honoring CLOUD Act requests.

The report also said that the U.K. Data Authority, the agency that oversees compliance with data protection law, has been slow to approve U.S. requests to share with other jurisdictions information the U.S. collected from U.K. providers under the agreement. The Justice Department and the Data Authority are in a tussle about what information the Justice Department needs to disclose to the Data Authority about the proposed onward transfer to warrant approval under U.K. law. Presumably, the Justice Department doesn't want to tell the Data Authority as much as the Data Authority wants to know.

Overall, the United States's light usage of the agreement should help assuage concerns in Europe and in other jurisdictions that agreements such as that of the CLOUD Act threaten to expand U.S. surveillance.

5. The agreement did not achieve the congressional objective of dissuading governments from passing dangerous surveillance laws (for example, those that threaten cybersecurity) and applying them to U.S. companies.

As reported in the press, the U.K. has sought to compel Apple to disable certain end-to-end encryption protection on all iPhone backups globally, which would make those backups available in plain text to U.K. authorities through the CLOUD Act agreement. Although the CLOUD Act requires that the report to Congress

include a description of "problems or controversies" arising from implementation of the agreement, the Justice Department report is silent about this extraordinary demand to Apple. This is perhaps because the department didn't know about it, or is respecting, U.K. requests for secrecy. Regardless, there's no doubt the Justice Department recognizes that had Apple complied, it too would benefit from this foreign law that could likely never have passed in the United States.

Tellingly, in the report, the Justice Department expresses surprisingly little concern about other recent troubling changes to U.K. surveillance law purportedly applicable to U.S. companies, saying that these changes "do not directly implicate" CLOUD Act criteria. When addressing concerns raised by providers, the report does acknowledge that providers warned the Justice Department about recent changes to U.K. law that, in combination with existing U.K. powers, could be used by U.K. authorities to "impede changes to privacy and security features that U.S. providers offer globally." This appears to be what the U.K. has done with Apple. It likewise cites the concern of an unnamed provider that the nondisclosure provisions in U.K. law restrict its ability to inform the Justice Department about U.K. practices. This is an issue that Jim Baker and I have raised before. In its report, the Justice Department takes a minimalist view of the significance of these sorts of issues when considering agreement renewal. It looks exclusively at commitments made in the agreement or orders, and in renewal criteria in the statute. Characterizing the provider concerns as irrelevant "to the [enumerated] statutory considerations in the CLOUD Act," the Justice Department casts them aside.

Recommendations

The report makes it clear that changes are needed if CLOUD Act agreements are to achieve the important objectives intended by Congress. A robust discussion of how to do this is essential. Below is a summary of priority recommendations for policymakers to consider.

Relieve the Burden of Mutual Legal Assistance

Before submitting an MLAT request, a CLOUD Act party should have at least attempted to invoke the CLOUD Act agreement to make requests. Since CLOUD Act requests aren't compulsory in themselves, some providers may decline to honor them. That means the MLAT process remains necessary, but it should be secondary. This could be implemented through a change to the CLOUD Act and in

each agreement to specify that the agreement serves as the primary mechanism for obtaining information covered by it, and that mutual legal assistance will be pursued only if the agreement process has failed or would clearly be futile.

Inhibit Extraterritorial Surveillance-Related Laws

Parties to CLOUD Act agreements should agree not to enact or enforce surveillance laws to regulate the providers in the other's jurisdiction or their subsidiaries. These surveillance laws include compulsory orders to disclose data. But the agreements should also prohibit adoption or enforcement of often-overlooked technical capability obligations, mandates to defeat or withhold security features, minimum data retention rules, and data localization requirements. In addition, the Justice Department should notify Congress of significant surveillance-related events that are relevant to the purposes of the CLOUD Act when it becomes aware of them, and not wait for the renewal date. Both of these can be implemented by specifying in the CLOUD Act that such laws are disqualifying and require notification to Congress, and in the agreement that enactment of such laws can result in immediate suspension or termination of the arrangement, or its nonrenewal.

Protect Cybersecurity

The U.S. should assert cybersecurity as a "national interest" in the CLOUD Act and in the agreements. In the event a party to an existing agreement takes action against a provider that would "significantly affect U.S. interests in ensuring U.S. companies follow responsible cybersecurity practices," as Sen. Alex Padilla (D-Calif.) and Rep. Zoe Lofgren (D-Calif.) wrote in their letter to the attorney general on this issue, the provider should be allowed to notify U.S. officials. The attorney general should then notify relevant committees (including the Senate and House Judiciary committees and the Senate Foreign Relations and House Foreign Affairs committees) and consider immediate action, in consultation with those committees. This too can be included in the CLOUD Act and the agreements.

Evaluate Efficacy

The reports to Congress are important, as even this rather cursory report demonstrated. These reports need to provide more information about the use of the agreement. Without more detail, it is impossible to know, for example, how many of the more than 20,000 wiretaps were of any real value, what categories of crime they covered, or how many Americans were swept up in the surveillance.

***

There's no doubt that, given the aggressive action by the U.K. authorities against Apple, there will be calls to abandon CLOUD Act agreements. That would be a mistake. The Justice Department report shows the potential of these agreements as a vehicle through which the U.S. can advance its national interests (like cybersecurity, reducing unnecessary burden on the MLAT system, and advancing the rule of law and human rights). Congress and the Justice Department need to make changes to achieve this potential, but it is in reach.

Richard Salgado

Read More

Richard Salgado teaches at Stanford and Harvard Law Schools. He also serves as an Advisory Board Member of American University Washington College of Law's Tech Law and Security Program, a Visiting Fellow on Security and Surveillance with the Cross-Border Data Forum, and a Senior Associate (Non-resident) with the Center for Strategic and International Studies. Richard founded a consultancy to provide guidance to organizations navigating cybersecurity and surveillance challenges. Richard has over 35 years of experience across the private sector, government and academia, including as Google's Director of Law Enforcement & Information Security for 13 years, and as a prosecutor with the Computer Crime and Intellectual Property Section of the Justice Department.