FOREIGN INFLUENCE ON AMERICAN'S DATA THROUGH THE CLOUD ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

OF THE

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

THURSDAY, JUNE 5, 2025

Serial No. 119–24

Printed for the use of the Committee on the Judiciary

Available via: *http://judiciary.house.gov*

U.S. GOVERNMENT PUBLISHING OFFICE

60–646 WASHINGTON : 2025

COMMITTEE ON THE JUDICIARY

JIM JORDAN, Ohio, *Chair*

DARRELL ISSA, California
ANDY BIGGS, Arizona
TOM MCCLINTOCK, California
THOMAS P. TIFFANY, Wisconsin
THOMAS MASSIE, Kentucky
CHIP ROY, Texas
SCOTT FITZGERALD, Wisconsin
BEN CLINE, Virginia
LANCE GOODEN, Texas
JEFFERSON VAN DREW, New Jersey
TROY E. NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
HARRIET M. HAGEMAN, Wyoming
LAUREL M. LEE, Florida
WESLEY HUNT, Texas
RUSSELL FRY, South Carolina
GLENN GROTHMAN, Wisconsin
BRAD KNOTT, North Carolina
MARK HARRIS, North Carolina
ROBERT F. ONDER, JR., Missouri
DEREK SCHMIDT, Kansas
BRANDON GILL, Texas
MICHAEL BAUMGARTNER, Washington

JAMIE RASKIN, Maryland, *Ranking Member*
JERROLD NADLER, New York
ZOE LOFGREN, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
ERIC SWALWELL, California
TED LIEU, California
PRAMILA JAYAPAL, Washington
J. LUIS CORREA, California
MARY GAY SCANLON, Pennsylvania
JOE NEGUSE, Colorado
LUCY MCBATH, Georgia
DEBORAH K. ROSS, North Carolina
BECCA BALINT, Vermont
JESÚS G. "CHUY" GARCÍA, Illinois
SYDNEY KAMLAGER-DOVE, California
JARED MOSKOWITZ, Florida
DANIEL S. GOLDMAN, New York
JASMINE CROCKETT, Texas

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

ANDY BIGGS, Arizona, *Chair*

TOM TIFFANY, Wisconsin
TROY NEHLS, Texas
BARRY MOORE, Alabama
KEVIN KILEY, California
LAUREL LEE, Florida
BRAD KNOTT, North Carolina

LUCY MCBATH, Georgia, *Ranking Member*
JARED MOSKOWITZ, Florida
DAN GOLDMAN, New York
STEVE COHEN, Tennessee
ERIC SWALWELL, California

CHRISTOPHER HIXON, *Majority Staff Director*
JULIE TAGEN, *Minority Staff Director*

C O N T E N T S

THURSDAY, JUNE 5, 2025

OPENING STATEMENTS

WITNESSES

LETTERS, STATEMENTS, ETC. SUBMITTED FOR THE HEARING

FOREIGN INFLUENCE ON AMERICAN'S DATA THROUGH THE CLOUD ACT

Thursday, June 5, 2025

HOUSE OF REPRESENTATIVES

SUBCOMMITTEE ON CRIME AND FEDERAL GOVERNMENT SURVEILLANCE

COMMITTEE ON THE JUDICIARY

Washington, DC

The Subcommittee met, pursuant to notice, at 10:05 a.m., in Room 2141, Rayburn House Office Building, the Hon. Andy Biggs [Chair of the Subcommittee] presiding.

Present: Representatives Biggs, Jordan, Tiffany, Nehls, Knott, Goldman, and Raskin.

Mr. BIGGS. The Subcommittee will come to order.

Without objection, the Chair is authorized to declare a recess at any time.

We welcome everyone to today's hearing on the CLOUD Act and foreign influence on America's data.

I now recognize the gentleman from Texas, Mr. Nehls, to lead us in the Pledge of Allegiance.

ALL. I pledge allegiance to the Flag of the United States of America, and to the Republic for which it stands, one Nation, under God, indivisible, with liberty and justice for all.

Mr. BIGGS. Thank you, Mr. Nehls. I now recognize myself for an opening statement.

I welcome my colleagues to this important hearing and welcome our audience and our witnesses today. I thank each of our witnesses for being here today, with special recognition for one of our witnesses who flew all the way from the U.K. to testify today. Thank you.

Given advances in technology and the heightened interconnectivity of the digital era, personal data, business information, and sensitive communications are sent, received, and stored all over the world.

Often during an investigation law enforcement needs to acquire this information from U.S. companies. Until 2018, if this information was held in another country—for example, a data server in Ireland—it wasn't clear whether U.S. law enforcement would be able obtain it, even though it was requesting the data from a U.S. company.

In 2018, Congress passed the Clarifying Lawful Overseas Use of Data Act, or the CLOUD Act, to address this gap in the law. Under the CLOUD Act, U.S. law enforcement, pursuant to a lawful court order, can obtain data held by U.S.-based service providers but stored outside of the United States.

The CLOUD Act also provides avenues for our allies to enter into bilateral agreements with the United States to similarly obtain their citizens' data from these same service providers to assist with their own law enforcement investigations.

Unfortunately, one of our closest allies, the United Kingdom, is taking advantage of its authorities under the CLOUD Act and is attacking America's data security and privacy.

In February of this year, *The Washington Post* reported that the U.K. had secretly ordered Apple to build a back door into its devices to enable U.K. law enforcement to access a user's data stored on the cloud, including encrypted data.

The CLOUD Act requires that a country entering into a data access agreement with the United States have laws that include robust protections for privacy and civil liberties. The U.K.'s order, however, threatens the privacy and security rights, not only of those living in the U.K., but of Apple users all over the world, including Americans.

This order sets a dangerous precedent and if not stopped now could lead to future orders by other countries. The U.K.'s Investigatory Powers Act permits it to issue orders to tech companies compelling them to weaken encryption or halt security updates for users around the world.

This broad extraterritorial order highlights the tension between national security and individual rights. These interests are not mutually exclusive, and it is possible to protect both national security and individual rights.

Providing law enforcement with the tools to conduct investigations is a laudable, important goal, but the U.K., seemingly emboldened by its agreement with the United States under the CLOUD Act, has issued an order that will affect people all over the world and this is a step too far.

Encryption is a critical tool to maintain the privacy and security of digital information and communications. Efforts to weaken or even break encryption makes us all less secure. The U.S.–U.K. relationship must be built on trust. If the U.K. is attempting to undermine this foundation of U.S. cybersecurity, it is breaching that trust.

If companies are forced to build back doors to encryption, that simultaneously opens a back door to privacy rights or an invasion of privacy rights.

It is impossible to limit a back door to just the good guys. Just last year, Chinese hackers known as Salt Typhoon penetrated lawfully mandated back doors, gaining access to wiretap systems used by U.S. law enforcement. The hackers also were able to access the private data of President Trump and Vice President Vance.

This attack is a clear example of the dangers of surveillance back doors. This should concern everyone. I've long had concerns about the CLOUD Act and the bilateral agreements it enables that could allow foreign governments to spy on Americans.

Given the recent actions by the U.K., I am concerned that the CLOUD Act is failing to adequately protect the privacy and security of Americans.

In the wake of the U.K.'s order, I have called on this administration to act decisively to protect Americans' communications.

I continue to urge our government, including the Justice Department, to evaluate whether the CLOUD Act and our agreement with the United Kingdom are working as intended.

If they are not, we should renegotiate the agreement to ensure that our rights are protected, and we should do so by invoking the 30-day termination clause.

After years of senior U.S. Government officials pushing for weaker encryption and surveillance back doors, it seems the tide has shifted. Indeed, after the Salt Typhoon hack, our government publicly recommended the use of end-to-end encrypted communications tools.

Director of National Intelligence Tulsi Gabbard stated at her confirmation hearing that back doors lead down a dangerous path that can undermine Americans' Fourth Amendment rights and civil liberties.

This hearing provides an opportunity to build on the momentum toward greater respect for privacy and evaluate whether and what changes are needed to ensure Americans' rights are protected.

I'm looking forward to hearing from our witnesses today—and, again, thank you for being here—and discussing how we can best move forward.

I now recognize the Ranking Member, Mr. Raskin, for his opening statement.

Mr. RASKIN. Mr. Chair, thank you very much. Welcome to our witnesses. I appreciate your being here with us.

Living in the digital age in America means that much of our connection with other people takes place over the internet. We message with friends and family and coworkers over our cell phone apps, we store documents in the cloud, and we share materials over email.

The end-to-end encrypted services promise that no one—not Apple, not Google, not the government, Federal, State, or local—can access the messages that we send. These platforms are increasingly counted on by users wishing for the privacy of a protected face-to-face conversation in the new era of technology that we inhabit.

Imagine pulling out your phone, opening up an app you've been told is secure, and sending a message to a friend. Now, imagine learning that the app is not end-to-end encrypted as promised. Instead, the government has ordered the service provider to make its security weaker so the government can demand access to your message. Imagine the government told the platform that they couldn't tell a soul about this arrangement.

Well, that's exactly what the United Kingdom secretly ordered Apple to do recently, and that's the reason that we're here today.

Requiring Apple to secretly build a so-called back door into its Advanced Data Protection service would make users' end-to-end encrypted documents no longer secure as expected. Law enforcement officers, not just in the U.K. but also in the U.S., could de-

mand Apple produce users' content and metadata from the cloud and cybercriminals would be able to exploit this system weakness introduced by the back door to target Americans for espionage, consumer fraud, and ransomware.

Back doors to encrypted technology are not capable, as the Chair said, only of letting good guys in while keeping the bad guys out. Back doors are intentionally designed weaknesses in an encrypted technology's mathematical formula.

These design weaknesses can be exploited by foreign governments seeking to compromise our national security, steal our intellectual property, and monitor us in our daily lives and workplaces.

Congress passed the CLOUD Act in 2018 to allow for data-sharing agreements between the U.S. and countries that meet required standards. Through its negotiated agreement with the U.S., U.K. law enforcement can access nonencrypted data transmitted by U.S. providers that is relevant to their law enforcement recommendations.

While secret orders like the Technical Capability Notice the Home Office placed on Apple have nothing to do with the data-sharing agreement or the CLOUD Act, they are only worthwhile to the U.K. because of the data that is made available through the agreement.

I, for one, believe that the CLOUD Act and the U.S.–U.K. data-sharing agreement thus far have been beneficial both to U.S. companies and to our country. I also believe that forcing companies to circumvent their own encrypted services in the name of security is the beginning of a dangerous slippery slope.

I look forward to hearing from the witnesses as to what, if anything, we need to do to change to prevent future similar orders against other companies.

Some argue that privacy is passe, yesterday's news. Cookies monitor which websites we click on, our devices already track every step we take, and data brokers take anonymized data and reidentify it in portfolios available to the highest bidder.

I disagree with the idea that privacy is no longer valuable or meaningful to the American citizenry. In a country where visa holders are being detained simply for opinions that they have expressed or an op-ed they wrote, where criticism of the administration can result in a visit from the Secret Services, and where the staff of Members of Congress can be arrested and handcuffed just for doing their jobs, Americans' security from government intrusion has never been more urgent or important.

The deluge of ways new technology enables the government to spy on their citizens makes it even more important that Americans stand up to increases in State surveillance.

Thomas Jefferson wrote in 1788 that,

> The natural progress of things is for liberty to yield and for government to gain ground.

Well, we have to resist that natural tendency.

A week ago, the Trump Administration announced it would hire Palantir to consolidate Americans' data into dossiers on all U.S. citizens.

The plan to use Palantir's Foundry project to organize and analyze data across agencies into one big, beautiful dossier is chilling.

It's the beginning of an effort to create a national citizen database, which would be vulnerable to manipulation, not just by outside actors, but by inside political actors.

From bank account numbers and student debt totals to medical claims and disability status, the administration today is taking information that was previously siloed into different categories, as required under the law, and using it to create one big, beautiful surveillance apparatus that can be used to crush resistance, to profile Americans, and to silence dissent.

We're here today to discuss the CLOUD Act. I recognize this. We should also recognize none of these issues exist in a vacuum. All government surveillance curtails all citizens' liberties.

It is not always immediate. Often it is a slow decay and erosion. Every chip in our civil liberties foundation brings us that much closer to a government that no longer has its foundational and necessary ideological checks against total control of the citizenry.

Surveillance databases like the one contemplated by the Trump Administration remain the stuff of science fiction and authoritarian governments, not a reality for a country founded on the principles of democratic self-government and freedoms and rights for the people.

In the case of the U.K. order, we can start with an easy first step. We don't need legislation to pass in the divided House or frozen Senate. The Trump DOJ can just do its job.

The U.S. should not sit idly by and watch the Home Office issue perhaps more secret orders against U.S. companies. Thus far, that's exactly what the DOJ has done. I sincerely hope that we move quickly to change that.

I thank Chair Biggs and Chair Jordan for holding a second bipartisan surveillance hearing, and I look forward to working across the aisle with my friends as we prepare for the expiration of FISA Section 702 next year.

I yield back to you, Mr. Chair.

Mr. BIGGS. The gentleman yields back. Thank you.

I now recognize the Chair of the Full Committee, Mr. Jordan, for his opening statement.

Chair JORDAN. No opening statement. I just want to thank the Chair for having this hearing, thank our witnesses for being here, and appreciate the remarks by both the Chair and the Ranking Member on this subject and the Ranking Member's reference to the work we have to do as 702 and the FISA come up for reauthorization less than a year from now.

With that, I would yield back to the Chair, and again thank our witnesses for being here.

Mr. BIGGS. I thank the Chair. The Chair yields back. Without objection, all other opening statements will be included in the record.

I'll now introduce today's witnesses.

With us today is Professor Susan Landau. Ms. Landau is a Professor of Cyber Security and Policy in the Department of Computer Science at Tufts University. Professor Landau's research focuses on privacy, surveillance, cybersecurity, and law.

She has previously worked or held faculty appointments at Google, Sun Microsystems, the Worcester Polytechnic Institute, the University of Massachusetts Amherst, Wesleyan University, the

National Academies of Sciences, Engineering, and Medicine, the National Science Foundation, and the National Institute of Standards and Technology.

Welcome, Professor. Thank you for being here.

Ms. Caroline Wilson Palow. Ms. Wilson Palow is the Legal Director and General Counsel at Privacy International, a nonprofit organization based in the U.K. Ms. Wilson Palow leads the organization's legal advocacy and advises its programs on legal strategy and risk.

Prior to joining Privacy International, she was an attorney with Wilson, Sonsini, Goodrich & Rosati, where her practice focused on privacy and intellectual property.

Thank you for joining us. Thanks for coming all this way, too.

Mr. Richard Salgado is the founder of Salgado Strategies, a consulting firm that advises clients on geopolitical, cybersecurity, and surveillance issues. He also serves as a lecturer at both Harvard Law School and Stanford Law School.

Mr. Salgado previously was the Director of Law Enforcement and Information Security at Google for more than 13 years, worked on international security and law enforcement compliance at Yahoo! and served in the Department of Justice.

Thank you, Mr. Salgado, for being with us.

Mr. Gregory Nojeim is a Senior Counsel and Director of the Security and Surveillance Project at the Center for Democracy and Technology, a nonprofit organization that advocates for civil rights and civil liberties in an increasingly digital world.

He previously served as the Associate Director and Chief Legislative Counsel of the ACLU's Washington office, where he focused on the civil liberties implications of terrorism, national security, and information privacy legislation.

We welcome all of you. Thank you for being here today.

We will begin now by swearing you in. Would you please rise and raise your right hand?

Do each of you swear or affirm under penalty of perjury that the testimony you are about to give is true and correct to the best of your knowledge, information, and belief, so help you God?

Let the record reflect that the witnesses have all answered in the affirmative.

You may now be seated. Thank you.

I want you to know that we've read your—I don't know, I won't guarantee everybody—but I've read your statements, and those will be entered into the record in their entirety. Accordingly, we ask that you summarize your testimony in five minutes.

At four minutes, the light should go yellow before you. When it's almost five minutes, I will just tap this a little bit so you'll know it's time to kind of wrap up. I don't want to cut you off too much, but we do want to remind you of that.

We thank you so much for being here.

Now, Professor Landau, I recognize you for your five minutes.

STATEMENT OF SUSAN LANDAU

Ms. LANDAU. Thank you, Chair Biggs, Ranking Member Raskin, and the Members of the Committee, for the opportunity to testify today.

I have no need to remind you of the damage caused by Salt Typhoon. I want to touch on the hackers' access to the databases of wiretap targets. This enabled the Chinese Government to learn which spies we had discovered.

It appears to have been made easier by the technical requirements and mandates imposed by the Communications Assistance for Law Enforcement Act. Introducing such access to complex systems—and communication systems are complex systems—increases security vulnerabilities.

At the same time, the Salt Typhoon hackers could not read communications sent through WhatsApp, Signal, or on Apple network. These were end-to-end encrypted, as the Chair mentioned, a form of cryptography which, as long as the communications device itself has not been hacked, only the sender and receiver can read the encrypted communication.

We all use end-to-end encryption daily. You almost always use it when you visit a webpage, you always do when you're sending credit card information. You use it on Signal, on WhatsApp, on multiple other applications.

Apple's Advanced Data Protection secures users' files by treating them as end-to-end encrypted messages sent from the user to themselves. Files are delivered when the user downloads them.

Meanwhile, they reside on the iCloud. Since only the user has the encryption key, the files cannot be decrypted while stored in the iCloud.

It is a terrific form of security. If there is ever a breach of the iCloud, the user's data is secure.

Who needs it? All of us. Journalists. Human rights workers. Members of civil society organizations. The latter are particularly targeted by Russia and China. Remote workers. Businesspeople while traveling. Members of your family with files they'd like to keep private, like healthcare proxies, wills, and financial information. Members of your staff. All of us.

Around the time the U.S. Government loosened export controls on encryption back in 2000, the NSA began encouraging wider use of strong encryption domestically. The FBI was less enthusiastic and began pressing about "Going Dark," its increasing inability to understand communications and later read files due to encryption.

The issue came to a head with the San Bernardino case involving a locked iPhone. Unable to open the device due to Apple's security protections, the FBI and DOJ sought to have Apple undo those protections.

Doing so was not nearly as straightforward as the FBI sought to portray. Requests for access were likely to be frequent, while information on obtaining access had to be stored for both legal and technical reasons. This created a serious security vulnerability and Apple refused to do it.

The case ended, by the way, when an FBI consultant was able to unlock the device.

The real point, though, is whether you're looking at CALEA, the 2016 fight over the locked iPhone, or the purported app the U.K. Technical Capability Notice served on Apple, these attempts at mandating lawful access to be built into complex communication

systems creates vulnerabilities in these systems. That's dangerous for Americans and for U.S. national security.

Protecting the private data of Americans is a critical aspect of protecting U.S. national security. This is because protecting the private communications of a CEO's son-in-law, the files of an American who has family working in China, the draft research papers of a graduate student in genomics who has not yet filed a patent on her work, is protecting both the individuals and the economic and national security of our Nation.

That's why former NSA Directors Mike McConnell and Michael Hayden, former DHS Secretary Michael Chertoff, former FBI General Counsel Jim Baker, and multiple other national security and law enforcement leaders support widespread public use of end-to-end encryption.

It is why the Chair mentioned the joint guidance of the governments of Australia, Canada, New Zealand, and the United States, post-Salt Typhoon, recommended that end-to-end encryption be used whenever possible for communications traffic to the maximal extent possible. By refusing to sign, the U.K. is a real outlier. It has become a "Four Eyes" statement.

Apple's advanced data encryption protects people's data. It is an important and needed technology. I urge you to ensure that the U.K.'s efforts to improve its own investigatory capabilities do not come at its expense.

The technology that Apple developed protects our national security and the security and privacy of ordinary Americans. It should be widely used and widely available. Please ensure that it continues to be so.

Thanks very much.

[The prepared statement of Ms. Landau follows:]

Testimony for
Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary
House of Representatives

Hearing on "Foreign Influence on Americans' Data Through the CLOUD Act"
June 5, 2025

Susan Landau, PhD
Professor of Cyber Security and Policy
Tufts University
177 College Ave.
Medford, MA 02155

Testimony for
Subcommittee on Crime and Federal Government Surveillance of the Committee on the Judiciary
House of Representatives

Hearing on "Foreign Influence on Americans' Data Through the CLOUD Act"
June 5, 2025

Mr. Chairman and Members of the Committee:

Thank you very much for the opportunity to testify today on "Foreign Influence on Americans' Data Through the CLOUD Act."

My name is Susan Landau, and I am Professor of Cyber Security and Policy at Tufts University. Until last September, I was Bridge Professor of Cyber Security and Policy at the Fletcher School of Law and Diplomacy and the School of Engineering, Tufts University. In this role, I initiated and directed a Masters program in Cybersecurity and Public Policy, run jointly between the two Tufts University schools. Previous to my time at Tufts University, I held positions as Professor of Cybersecurity Policy at Worcester Polytechnic Institute, Senior Staff Privacy Analyst at Google, and Senior Staff Engineer and Distinguished Engineer at Sun Microsystems. I have also held academic positions at the University of Massachusetts, Amherst and at Wesleyan University. I hold a PhD in applied mathematics from MIT, an MS from Cornell University, and a BA from Princeton University.

I have studied and written about the security and privacy of communications systems for over thirty years. My scholarship has focused on the security threats posed to communications systems by "lawful access" to encryption and communications networks public policy issues. In this context, I have testified before the U.S. Congress and served on study committees focusing on privacy, surveillance, and encryption issues for the National Academies of Science, Engineering, and Medicine, the Carnegie Endowment for International Peace, and other organizations.

My comments today are on my own behalf and do not represent my employer or any other organization. My testimony is focused on the technical issues raised by the U.K.'s Technical Capability Notice and its application to Apple's Advanced Data Protection for iCloud; I have left the legal and policy issues to the other witnesses at today's hearing.

Apple's Advanced Data Protection for iCloud and the U.K.'s Technical Capability Notice

As the committee knows, in February the *Washington Post* reported that Apple had been told by the U.K. government to provide access to encrypted iCloud material regardless of the data's location. Under the purported order, the Technical Capability Notice of the Investigatory Powers Act (TCN) would require Apple to:

provide and maintain the capability to—
(a) disclose the content of communications or secondary data in an intelligible form where reasonably practicable;
(b) remove electronic protection applied by or on behalf of the telecommunications operator to the communications or data where reasonably practicable.

The TCN was purportedly targeted at Apple's Advanced Data Protection for iCloud (ADP) and would require that Apple be able to decrypt data stored using ADP.

As I shall explain in a moment, that is a contradiction in terms. It also goes against the security protections needed in the face of sustained and increasingly sophisticated cyberattacks by nation-state adversaries. I will begin by briefly explaining the meaning and use of end-to-end encryption, then describe Advanced Data Protection.

End-to-End Encryption and Apple's Advanced Data Protection System

End-to-end encryption is a form of cryptography in which *only the sender and the receiver can read the encrypted communication*. All of us—members of Congress, their family members, their staff, me, my students, and anyone who uses the Internet uses end-to-end encryption multiple times a day. If you visit a webpage, chances are high—88% at present[1]—that your communication to the page, which could be your credit-card number, or the page's communication to you, which could be about your investments—are both using end-to-end encryption. If you send a text message from one iPhone to another, you're using end-to-end encryption. If you use Signal for an email or a phone conversation, you're using end-to-end encryption.

Apple's Advanced Data Protection (ADP) is designed to provide end-to-end encryption with a user-supplied key. It is an end-to-end encrypted message sent by the user to themselves, with the data temporarily residing on the iCloud. The iCloud doesn't have a key to the encrypted data. If a user opts in to use ADP, the user's data stored in the iCloud can only be decrypted on the user's devices. When the user's data is downloaded onto one of the user's devices, it can be decrypted. But it cannot be decrypted elsewhere.

This point bears repeating: Apple designed ADP so that the user's devices—*and only the user's devices*—have unencrypted access to the user's data stored in the iCloud. This is a terrific form of security. Apple can't read the user's files. Neither can anyone else. If there is ever a breach of iCloud, the user's data is secure. That is, in a breach, criminals would be able to download the data, but they wouldn't be able to read it. The content would be encrypted gibberish.

Let me note here that while the content of end-to-end encrypted communications is encrypted, the communications metadata—who communicated with whom when and from where—is

[1] Web Technology Surveys, "Usage statistics of default protocol https for websites," https://w3techs.com/technologies/details/ce-httpsdefault.

typically not. Such information can be remarkably revelatory[2] and has become the backbone of national-security and law-enforcement investigations.

Why End-to-End Encryption—and its Implementation in ADP—are Important

Recently the National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) recommended that "Ensure that [communications] traffic is end-to-end encrypted to the maximum extent possible."[3] This marked a notable change in U.S. policy. The reason was the insecurity of our communication networks and the continuing unrelenting assaults by our adversaries.

Last fall we learned about the discovery of Salt Typhoon, the intrusion into U.S. telecommunications networks that has been widely attributed to Chinese government hackers.[4] Though we have known about vulnerabilities in the telecommunications networks for some time, we didn't act—or didn't act sufficiently. Salt Typhoon took advantage of these insecurities. This intrusion, done with great care and secrecy, demonstrated the damage that can occur when a communications network is penetrated.

The hackers are said to have collected communications from President-elect Donald Trump, Vice-President-elect JD Vance, members of the Harris campaign, and members of Congress. They accessed the databases that carriers used for legally authorized wiretaps, allowing the Chinese government to know which of their spies were under surveillance. And they also accessed millions of call metadata records—who called whom when—information that gave the Chinese government information enabling them to develop detailed records of millions of Americans. That's detailed records of journalists who might later be posted to Beijing, detailed records of Chinese students studying in the U.S., detailed records of members of the Chinese diaspora who might still have family in the People's Republic. The result is a treasure trove of personal information that can later be exploited, potentially creating damage for many years to come. As I have discussed elsewhere,[5] Salt Typhoon exemplifies the security risks of government mandates that, to ease evidence collection by law enforcement, introduce vulnerabilities into the system.

Our computer and communications systems remain under constant attack. While some of the problems that allowed the Salt Typhoon cyberexploit to occur can be corrected, not all can be. Communications networks are complex systems. As a National Academies of Science study

---

[2] Susan Landau, "Transactional information is remarkably revelatory," *Proceedings of the National Academy of Sciences* 113(20), pp.5467-5469.
[3] U.S. Cybersecurity and Infrastructure Security Agency, U.S. National Security Agency, U.S. Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Cyber Security Centre, New Zealand's National Cyber Security Centre, *Enhanced Visibility and Hardening Guidance for Communications Infrastructure*, Dec. 4, 2024, https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure, 4.
[4] Sarah Krouse, Dennis Volz, Aruna Viswantha, and Robert McMillan, "U.S. Wiretap Systems Targeted in China-linked Hack," *Wall Street Journal*, Oct. 4, 2024.
[5] Susan Landau, "The Dangers Lurking in the U.K's Plan for Electronic Eavesdropping," *Lawfare*, Feb. 25, 2025, https://www.lawfaremedia.org/article/the-dangers-lurking-in-the-u.k.-s-plan-for-electronic-eavesdropping.

observed over a quarter of a century ago, complex systems are insecure.[6] The former NSA Director of Research, Fred Chang, reiterated that point a dozen years ago in testimony in a hearing before the House Committee on Space, Science, and Technology, stating, "When it comes to security, complexity is not your friend. Indeed it has been said that complexity is the enemy of security."[7]

Protecting the security of communications is basic for the security of our country. Communications—whether between campaign managers and presidential candidates, chip engineers and software designers, members of a research team investigating a new virus, or town officials considering a zoning change—must be protected.

Just as communications must be secured, so must data. The problem is one we didn't have when information—business records, financial records, medical records, school records, private communications—was stored in manila folders in wooden file cabinets. Now our model of work is no longer tied to the office with its file cabinets; we travel with our electronic devices and anticipate being able to access such data, confidential or merely private, and use those devices while outside our office or home. And it is not just users with security clearances that need strong protections for their data. A remote worker needs to know her documents in the cloud are secured from snoopers as she transits borders. Journalists, human rights workers, and other members of civil society need to be able to keep their files secure from spies, foreign and domestic. The politician's daughter wants assurance that the photos of her and her lover are protected against the efforts of those who might want to embarrass her father.[8]

For decades, technologists have been making the point that the strongest form of communications security is provided by end-to-end encryption.[9] The Salt Typhoon hack provided an example of this. Because WhatsApp, Signal, and messages sent via Apple's networks were protected by end-to-end encryption, the Salt Typhoon hackers were unable to read those communications.

ADP extends the protections of end-to-end encryption to data the user stores in the iCloud. It is a clever solution—for users who need access to their data while on the move (Google also has this technology). The security needs that ADP fills are for all of society. And yes, the bad guys will use this too and thus be harder to catch. But blocking the masses from access to good security tools to simplify the catching of criminals, the best of whom would nonetheless find ways to thwart surveillance, is poor public safety practice.

---

[6] Fred B. Schneider, ed., *Trust in Cyberspace* (National Academies Press, 1999), 110.
[7] "Is your data on the Healthcare.gov website secure?," Hearing before the House Committee on Space, Science, and Technology, 113th Congress, First Session (statement of Frederick R. Chang, professor, Southern Methodist University).
[8] Some of the text in this paragraph previously appeared in Susan Landau, "The Dangers Lurking in the U.K.'s Plan for Electronic Eavesdropping," *Lawfare,* Feb. 25, 2025, https://www.lawfaremedia.org/article/the-dangers-lurking-in-the-u.k.-s-plan-for-electronic-eavesdropping.
[9] For example, IBM states, "End-to-end encryption (E2EE) is widely considered the most private and secure method for communicating over a network." IBM, "What is E2EE?," https://www.ibm.com/think/topics/end-to-end-encryption.

Currently, Apple is partially complying with the TCN order by removing Advanced Data Protection for U.K. users, while continuing the use of the technology for users outside the U.K. That is, users in the U.K. no longer have the option of Advanced Data Protection, while users outside the nation continue to do so.

Were the TCN to be applied in its full strength to Apple's ADP program, Americans would no longer have access to an Apple product that provides end-to-end encryption for data users store in the iCloud. That means that to protect the security and privacy of their information, the commuter, the business traveler, and the vacationer must give up convenience—storing data to be accessed on their various devices—or security. The latter makes no sense when the skills and cyber heists of our adversaries are increasing—and when they have shown themselves to be increasingly interested in collecting private data about private individuals. That's why the U.K.'s Technical Capacity Notice is so problematic.

Building in Lawful Access is Building in a Security Vulnerability

For decades, law enforcement has been seeking a way to build in legally authorized access to encrypted communications. Law enforcement may call this "lawful access," but what it really is is an architected security breach—and it's dangerous. I will provide a few examples of where such access has shown serious security problems.

In the 1990s, the U.S. government proposed the Clipper chip, a system in which the keys were split and held in two agencies of the federal government.[10] It was a failure. Opponents included a large segment of the computer industry, various federal agencies, including the Department of Energy and the Nuclear Regulatory Commission, and civil-liberties organizations. Objections varied from the bureaucratic hurdles the government had erected by regulating which companies could include the technology in their products to security risks it would cause to issues of privacy. And foreign governments, not surprisingly, didn't like the system one bit.

But the most serious problem with Clipper was security. The system introduced a potential third party to a communication: anyone with access to the key-recovery system. The most serious issue would be the operational complexity needed to run the system: seventeen thousand federal, state, local, and tribal police forces would be using the system. Users would have to be authenticated, as would many other aspects of the access request, including court orders, validity of the dates, etc. Such complexity is the bane of security.[11]

Concentrating decryption keys in a central location would create a rich target for an adversary, especially one with the capabilities of a nation-state. There would be danger of an insider attack, especially given the richness of the information that would be revealed. And the system would prevent the use of *forward secrecy*, a technology used in communications systems that prevents a key exposure from enabling decryption of all previously encrypted communications.

---

[10] Computer Security Division, National Institute of Standards and Technology, "Escrowed Encryption Standard," Federal Information Processing Standard 185, Feb. 9, 1994, withdrawn Oct. 19, 2015.
[11] Hal Abelson et al. "The risks of key recovery, key escrow, and trusted third-party encryption," *World Wide Web Journal* 2, 3 (1997): 241-257

AT&T built the devices with the Clipper Chip, expecting to have a mass market item that businesspeople would travel with to ensure secure communications. A year into the project, the company had sold a total of 17,000 phones, of which 9,000 were sold to the FBI "in an attempt to seed the market."[12] The market spoke. The Clipper Chip was a failure, both as a product and because it helped to delay the deployment of strong forms of encryption in consumer devices.

Another example had its genesis with the U.S. export controls on encryption in the 1990s. These controls permitted license-free exporting computer and communication devices with encryption systems using 40-bit keys; anything with a longer key needed an export license, which was often not granted. Before I go into the problem, I'll briefly explain the issue of 40 bits and strength of cryptosystems.

A cryptosystem is considered secure if it is effectively resistant to any methods for breaking it short of "brute force," that is, trying all possible keys and the brute-force attacks must be infeasible. To use brute force to find the 40-bit key would require testing *all* 2^{40}, or approximately one trillion, possible keys. By the early 1990s, encryption systems with 40-bit keys were considered insecure since computers of the time could execute 2^{40} instructions in an hour.

U.S. export controls on encryption are much looser now, but the controls on devices with keys of 40-bits left a legacy that led to a security vulnerability, one that hid for over a decade. This is due to communications system being "backwards compatible," which allows an old communications device to still connect even as new capabilities appear. Thus, the phone your parents had when you were growing up must be able to take and make calls to a mobile phone and allows a browser satisfying the 1990's export controls to access a webpage even if the out-of-date browser can't display the dancing pigs on the site. To do this, a widely used network communications protocol is designed to be *backwards compatible* with older versions.

Once U.S. export controls were loosened in 2000, this communications protocol could use much longer encryption keys.[13] But for backwards compatibility, the protocol had a feature to allow it to "rollback" to an export-control version. In 2015, academic researchers found a vulnerability that enabled fooling a site into believing the visitor's browser was using the export-control version of the protocol. That is, even though both the site and the user's browser were set to use strong encryption, the researchers found a way to cause use of the short keys satisfying the 1990s export controls. Then, by doing a computation of a few hours on the keys, the researchers could decrypt the connection.[14] The situation was quite bad. Because the same key was often used for

---

[12] Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press (rev. ed. 2007), 239.

[13] This was Transport Layer Security ("TLS"), the protocol that provides security for communications over the Internet. Secure browser connections (https) use TLS, as do such email applications as Outlook, Gmail, MacMail, and Thunderbird. If your communication is protected by TLS and someone is listening in, they will be able to learn which website you are visiting or what application you are using (e.g., browsing, email, Voice over IP), but not what you are looking at or what the mail or conversation says.

[14] The 40-bit requirement described above was for symmetric, or "private-key," encryption; the part of the protocol attacked used "public-key" encryption, in which different keys are used for encryption and decryption. Public-key and private-key systems have different properties. In particular, for effectively the same security, public-key systems use longer key lengths than private-key systems. So the license-free export control limit in the 1990s was 512-bt

all connections to the server until the server was rebooted, this breach in confidentiality could go on for days.

At the time this research was done, 36% of servers were vulnerable to this attack.[15] A hacker collecting communications to and from a site with this vulnerability could thus decrypt the communications they collected. Sites that were vulnerable included www.nsa.gov, tips.fbi.gov, jcpenney.com, jcrew.com, umich.edu—and 5 million others.[16] We don't know if communications from those sites were hacked and whether, for example, organized criminals learned what tips were being provided to the FBI or criminals penetrated communications with J.Crew and thus learned customers' credit-card information. But we do know that a software vulnerability combined with the need for backwards compatibility for the browser and a woefully weak encryption key used in the 1990s resulting from export controls combined to leave a major security hole for all users.

Yet another example of law-enforcement access requirements resulting in vulnerabilities occurred because of the1994 *Communications Assistance for Law Enforcement Act* (CALEA). This law required that all digital communications switches be wiretap enabled. Computer scientists repeatedly warned that CALEA was a severe security risk.[17] Indeed, when the NSA examined CALEA-compliant switches for use by the Department of Defense, every single switch tested had a security flaw.[18]

No surprise then, that CALEA-compliant or CALEA-like switches were broken into. One known example of this concerned a Greek Telecom switch in Athens. This had a wiretapping interface that complied with European Telecommunications Standards modelled on CALEA. Private communications of 100 senior members of the Greek government, including the prime minister, the head of the opposition, and the heads of the Ministry of Interior and Ministry of Defense, were wiretapped by parties unknown for 10 months in 2024-2005.[19] I testified before the House Judiciary committee in 2016 in a hearing on encryption and the San Bernardino case; at the time, I was told that the U.S. Intelligence Community knew of other instances of breaks into CALEA

---

keys for public-key systems. The search for the decryption key in the public-key system was more complex than the brute-force system and took about seven hours, rather than one hour cited in the text for searching through 2^{40} keys. See: B. Beurdouche et al., "A messy state of the union: Taming the composite state machines of TLS. In IEEE Symposium on Security and Privacy, 2015.

[15] Matthew Green, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')," A Few Thoughts on Cryptographic Engineering, Mar. 3, 2015, https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/.

[16] Matthew Green, "Attack of the week: FREAK (or 'factoring the NSA for fun and profit')," A Few Thoughts on Cryptographic Engineering, Mar. 3, 2015, https://blog.cryptographyengineering.com/2015/03/03/attack-of-week-freak-or-factoring-nsa/ and "Tracking the FREAK Attack," https://freakattack.com/.

[17] See, e.g,, Susan Landau, "CALEA was a National-Security Disaster Waiting to Happen," *Lawfare*, Nov. 13, 2024, https://www.lawfaremedia.org/article/calea-was-a-national-security-disaster-waiting-to-happen for a discussion of some of these.

[18] Private communication with Dickie George, former NSA Technical Director for Information Assurance, Dec. 1, 2011.

[19] Vasilos Prevelakis and Dmitri Spinellis, "The Athens Affair," *IEEE Spectrum* 44, No. 7 (2017).

and CALEA-like systems. And, of course, Salt Typhoon broke into the CALEA databases of targets.

These are some of the cases of publicly known breaches that resulted from efforts to enable lawful access into communications systems. Building access into communications protocols or networks weakens security. This is not a mathematical theorem. It stems from lawful access into communication networks making complex systems even more complex —with complexity being the bane of security.

The Security Risks of the U.K TCN Requirement

As I noted earlier, the TCN is a contradiction in terms. The U.K. government maintains that compliance with the TCN can be achieved while still leaving a product fully secure. In this, the U.K. government is pursuing a pipe dream: end-to-end security of data with lawful access.

Apple describes ADP as a privacy feature—and it is—but it is also a security feature. ADP secures the user's data. However, the U.K. government doesn't see the technology as a form of security, but rather as an inappropriate impediment to the government's ability to conduct legally authorized investigations.

It's no accident that the U.K. requirement comes as a law and not as a technology. As technologists, we've had repeated requests from law enforcement to develop secure communications with access for legally authorized wiretaps, a technology sometimes called "exceptional access," since the 1990s. No one explains how exceptional access would actually work. Instead, we're told that surely the smart technologists can figure it out. But the real reason for the lack of specific proposals from government is the exceptional difficulty of providing access without introducing major security problems.

Maybe the proposed solution makes an assumption about the security of software updates that won't hold up in the face of an attack by a nation-state. Such updates were behind the Russian Solar Winds cyberattack.

Or the solution has a serious technical flaw, such as it breaks *forward secrecy*, a technology employed by major tech companies, or *authenticated encryption*, a technology that simultaneously provides confidentiality and authenticates the sender.[20]

Perhaps the solution fails to work at scale (a common issue for technologies that look promising when tested on 100,000 devices and totally fail when the network is at 100 million).

Or maybe the technology can be easily repurposed so that it would be used, not only finding evidence of say, Child Sexual Abuse Material (CSAM), but other forms of content that are legal but authorities would prefer to restrict.[21]

---

[20] Harold Abelson et al., "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity* 1, 1 (2015), 69–79.
[21] Harold Abelson et al., "Bugs in our pockets: the risks of client-side scanning," *Journal of Cybersecurity* 10, 1 (2024).

Ten years ago, I wrote that, "The problem is that once one gets into the nitty gritty of how exceptional access [to encrypted communications] might actually work, the idea of exceptional access looks more like magical thinking than a realistic solution to a complex technical problem."[22] Those words are still true today.

The TCN situation bears striking similarities to the situation in the 2016 San Bernardino case in which Apple and the FBI were in a legal and policy battle over a locked terrorist iPhone. The Bureau believed that the phone might hold crucial investigative information, but Apple's secure-by-default data protection system prevented the FBI from unlocking the device. FBI Director James Comey pressed hard for Apple to undo the security system and unlock the device, claiming that only Apple had the capability to get around the security protections. The Department of Justice (DoJ) argued similarly in court. As it turned out, both the Director and DoJ were wrong; an FBI contractor was able to exploit a vulnerability on the iPhone and unlock the device. This is, in fact, the business that Cellebrite, Graykey and multiple other companies are in—reiterating the point that complex systems have vulnerabilities.

Apple's court brief, based in part on testimony I provided before Congress,[23] was that the creation of such software and its usage would result in a security vulnerability. The access capability would be likely to be used frequently, while the information on how to obtain access would need to be documented in Apple systems for both legal and technical purposes. Those two reasons, plus the possibility of insider threat, created a serious security risk. Similar risks would arise for architecture to comply with the TCN requirement.

The U.K. government should know better about the difficulty of backdooring end-to-end encryption. In the 1990s, wiretapping needs centered on organized crime, terrorists, drug dealers, and kidnappers. By the 2010s, there was increased law-enforcement focus on online sharing of Child Sexual Abuse Material (CSAM).

One proposal for preventing such online sharing of illicit material while still enabling secured communications was "Client-Side Scanning." This proposed technology, which Apple had, in fact, begun to develop and then abandoned, worked on the premise that scanning photos on a user's phone prior to including them in an encrypted message, was both secure and not privacy invasive. As my colleagues and I showed, this was implausible—and dangerous, as such technology can be repurposed for other uses by authoritarian governments.[24]

Yet in late 2021, the U.K. government launched a "Safety Tech Challenge" of research awards of £85,000 to "to prototype and evaluate innovative ways in which sexually explicit images or

---

[22] Susan Landau, "Keys under Doormats: Mandating Insecurity," *Lawfare*, Jul. 7, 2015, https://www.lawfaremedia.org/article/keys-under-doormats-mandating-insecurity.
[23] "The Encryption Tightrope: Balancing Americans' Security and Privacy," Hearing before the House Committee on the Judiciary, 114th Congress, Second Session (statement of Susan Landau, professor, Worcester Polytechnic Institute), 104-130.
[24] Harold Abelson et al., "Bugs in our pockets: the risks of client-side scanning," *Journal of Cybersecurity* 10, no. 1 (2024). (Arkiv version: https://arxiv.org/pdf/2110.07450, Oct. 15, 2021.)

videos of children can be detected and addressed within end-to-end encrypted environments."[25] To put it bluntly, this challenge was nonsense: end-to-end encrypted messages reveal nothing about the content of a message except its length.

The team evaluating the outcomes of the five funded projects were only partially successful in doing so as their hands were tied: they were not given access to the experimental data of the projects.[26] Thus, they were unable to evaluate the percentages of false positives or false negatives or the scalability of the proposed technologies.[27] But the most important conclusion was that the confidentiality of end-to-end encrypted communications cannot be guaranteed if all content to be sent is monitored pre-encryption.[28] Also damning was the evaluators' observation that "transparency, disputability and accountability proved to be problematic in most of the tools."[29] In short, the U.K. government appears to be enforcing a law that it already has reason to believe involves capturing a chimera.

End-to-end encryption is the only way to secure a communication between two parties. Of course, if one of the parties' devices is insecure (e.g., a wiretapping capability has been placed on it), then the communication will not be secured. But otherwise, end-to-end encryption provides security to communications—and thus to the data the user has stored in the iCloud—in a way that no other technology can assure. Apple's ADP is an appropriate solution for the security and privacy threats members of the public face.

The Fight over Encryption

Over the last several decades U.S. national security and law enforcement have moved from opposing widespread public access to strong encryption to supporting it. Because these changes illuminate the value our national-security and public-safety leaders see in end-to-end encryption, I'd like to end my testimony with a brief reprise of that history.

In the early 1970s, academic and industry research scientists began thinking about solutions for how to secure communications. The answer is, of course, encryption. It is the only technology that can fully protect the confidentiality of accessed data. This new-found interest in cryptography by industry and academia was disturbing to the intelligence community (IC), which previously had been effectively the sole players in this field, and initially the IC tried to dampen non-governmental work in the field.

---

[25] Business Connect, "Safety Tech Challenge Fund," https://iuk-business-connect.org.uk/opportunities/safety-tech-challenge-fund/.

[26] Claudia Peersman et al., *Towards a Framework for Evaluating CSAM Prevention and Detection Tools in the Context of End-to-end encryption Environments: a Case Study,* REPHRAIN 2022, https://www.rephrain.ac.uk/wp-content/uploads/Safety-Tech-Challenge-Fund-evaluation-framework-report-1.pdf.

[27] Ibid.

[28] Ibid.

[29] Ibid.

In the late 1970s, NSA briefly sought to prevent the publication of academic research in cryptography. In the mid-1980s, the agency sought to control the development of public standards within the United States. Neither occurred. In the1990s, the U.S. and E.U. prevented the deployment of strong encryption—encryption effectively unbreakable by the computers of the era—through export controls. But then the situation began to change.

Computers' increasing speed of computation made adopting strong forms of encryption for military and government communications easy for all nations, not just technically advanced ones. At the same time, U.S. export controls were problematic for the computer industry, which feared losing business to nations that could deploy strong encryption within their exportable computer and communications systems.

Because of the changes in use of encryption by foreign governments, NSA was turning its focus to computer network exploitation (CNE), extracting information from computer networks. So effectively, the agency made a deal: a liberalization of the cryptographic export controls and increased NSA funding for CNE work. Though the export controls that mattered most to NSA remained,[30] controls that most concerned industry were lifted, enabling far simpler export of U.S. products with strong encryption. This had the not-unexpected side effect that it was far simpler to develop such products for the U.S. domestic market. This benefitted the DoD, which is required by the Clinger-Cohen Act to use Commercial Off the Shelf (COTS) products for DoD communications and computer equipment.[31] As the DoD knows, use of COTS is also good security practice. Industry's speed of innovation provides DoD with cutting edge technology; thus, for example, iPhones and iPads were cleared for DoD use in 2013.[32]

While national intelligence agencies understood the tradeoff that liberalizing export controls involved and were willing to live with the bargain, U.S. law enforcement was unhappy with the result. By the late 2000s, the FBI began speaking publicly about "Going Dark": being unable to access legally authorized wiretaps. Law enforcement in the U.S., U.K., and E.U. repeatedly pressed for laws that would require companies to provide access to encrypted communications. The need for encrypted communications and secured data was also a public safety issue, a point that privacy experts, journalists, and human rights workers made repeatedly. And by the mid 2010s, members of the national-security community began speaking publicly about the value of encrypting communications, including the use of end-to-end encryption.

In a 2015 *Washington Post* op-ed, former NSA Director Mike McConnell, former Secretary of Homeland Security Michael Chertoff, and former Deputy Secretary of Defense William Lynn III wrote, "We believe the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring."

---

[30] These were custom-designed systems, and systems for foreign governments and foreign communications providers.
[31] The Act requires use of COTS wherever feasible.
[32] Defense Information Systems Agency, "DISA Approves STIG for Government-Issued Apple iOS 6 Mobile Devices," May 17, 2013, https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=4641.

In 2016, during an interview on PBS News Hour, former director of NSA and CIA Michael Hayden said, "American security is better served with end-to-end encryption."

Jim Baker was FBI General Counsel at the time of the Apple/FBI case and helped craft some of the arguments that the FBI pursued in 2016. But as cybersecurity threats changed, Baker, no longer at the FBI, changed his view:

> One of the most important cybersecurity risk factors is that digital isolationism is not possible. Governments, corporations and individuals in the United States and other democratic societies communicate regularly with people all over the world. Civilian and military governmental organizations operate worldwide, as do all major transnational corporations.
>
> As a result, many communications vital to the security and well-being of the United States are, and increasingly will be, transmitted via telecommunications equipment that is manufactured and operated by foreign companies over which the U.S. government has insufficient control in light of the risks involved.
>
> …
>
> In light of the serious nature of this profound and overarching [cybersecurity] threat, and in order to execute fully their responsibility to protect the nation from catastrophic attack and ensure the continuing operation of basic societal institutions, *public safety officials should embrace encryption.* They should embrace it because it is one very important and effective way—although certainly not the only way and definitely not a complete way—to enhance society's ability to protect its most valuable digital assets in a highly degraded cybersecurity environment.[33]

With Salt Typhoon, those risks have come to pass, though not precisely as Baker envisioned. And thus the U.S. Cybersecurity and Infrastructure Security Agency, NSA, the FBI, the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Cyber Security Centre, and the New Zealand National Cyber Security Centre issued guidance that included the recommendation, "Ensure that traffic is end-to-end encrypted to the maximum extent possible."[34] The importance of widespread use of end-to-end encryption by the public is now a settled debate, although the U.K., the fifth member of the Five Eyes, is a notable outlier.

---

[33] Jim Baker, "Rethinking Encryption," *Lawfare*, Oct. 22, 2019, https://www.lawfaremedia.org/article/rethinking-encryption.

[34] U.S. Cybersecurity and Infrastructure Security Agency, U.S. National Security Agency, U.S. Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Cyber Security Centre, New Zealand's National Cyber Security Centre, i*Enhanced Visibility and Hardening Guidance for Communications Infrastructure*, Dec. 4, 2024, https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure, 4. Though the FBI signed onto this guidance, on its webpages, the Bureau states, "Law enforcement supports strong, responsibly managed encryption. This encryption should be designed to protect people's privacy and also managed so U.S. tech companies can provide readable content in response to a lawful court order. "Lawful Access: Myth vs. Reality," https://www.fbi.gov/about/mission/lawful-access/lawful-access-myths-vs-reality.

I will end by noting what Ciaran Martin, who headed the U.K.'s National Cyber Security Centre, wrote after he left government service, "If cyber security were the sole objective of government technology policy, end-to-end encryption would enjoy unqualified Government support."[35]

Protecting the private data of ordinary Americans is a critical aspect of protecting U.S. national security. And I believe, as Jim Baker does, that our cybersecurity threats are such that they exceed the need for faster resolution of law-enforcement investigations. That is why the joint guidance issued by the governments of Australia, Canada, New Zealand, and the United States recommended that end-to-end encryption be used for communications traffic to the maximal extent possible.[36]

I urge you to ensure that the U.K.'s efforts to improve its own investigatory capabilities do not come at the expense of Advanced Data Protection. The technology that Apple has developed protects our national security and the security and privacy of ordinary Americans. It should be used, and additional protective technologies like this should be developed.

Thank you.

---

[35] Ciaran Martin, *End-to-End Encryption: The Fruitless (?) Search for a Compromis*e, lecture delivered at Bingham Centre for the Law, November 2021, 6, https://www.bsg.ox.ac.uk/sites/default/files/2021-11/End-to-end%20Encryption%20Ciaran%20Martin%20Blavatnik%20School.pdf.

[36] U.S. Cybersecurity and Infrastructure Security Agency, U.S. National Security Agency, U.S. Federal Bureau of Investigation, Australian Signals Directorate's Australian Cyber Security Centre, Canadian Cyber Security Centre, New Zealand's National Cyber Security Centre, *Enhanced Visibility and Hardening Guidance for Communications Infrastructure*, Dec. 4, 2024, https://www.cisa.gov/resources-tools/resources/enhanced-visibility-and-hardening-guidance-communications-infrastructure, 4.

Mr. BIGGS. Thank you. Now, I recognize you, Ms. Wilson Palow, for your five minutes.

STATEMENT OF CAROLINE WILSON PALOW

Ms. WILSON PALOW. Thank you, Chair Biggs, Ranking Member Raskin, and the Members of the Subcommittee. Thank you for the opportunity to testify today on behalf of Privacy International.

I'm here to tell you about a troubling surveillance power that allows the United Kingdom's government to secretly order a U.S. company to undermine the security, privacy, and free speech rights of Americans.

Indeed, due to the global reach of U.S. companies, these orders threaten the security and fundamental rights of users worldwide.

This power can be found in the U.K.'s Technical Capability Notice regime, which is part of the Investigatory Powers Act of 2016.

Under this law, the U.K. can order a telecommunications service provider to build or modify its systems so that in the future the U.K. can access data on those systems through other lawful processes, such as warrants authorizing the interception of content or overseas protection orders permitted under the CLOUD Act. More on that later.

I have provided a more detailed description of these notices in my written statement. In brief, the most salient aspects of them are that they are ill-defined, secret, and extraterritorial. American companies subject to a U.K. order cannot reveal even its existence to U.S. officials and oversight bodies, much less users, investors, or anyone else who plays a crucial role in vetting the legality and wisdom of such notices.

Why are we concerned about a U.K. surveillance power affecting American companies? Because these notices can be given to companies outside of the U.K. so long as the company offers, provides, or controls services used by people in the U.K. This small nexus is sufficient for the U.K. to demand a company change its systems worldwide, affecting all its users, whether in the U.K., the U.S., or elsewhere.

We are here today because in February *The Washington Post* revealed that a U.S. company, Apple, received a secret notice requiring it to undermine the security of its Advanced Data Protection service, as Professor Landau has described, which is an optional security feature for Apple's users providing end-to-end encryption of iCloud storage that only the iCloud user, not Apple itself, can unlock.

The Washington Post reporting and the significant press followup have provided us with a potentially unique opportunity to have a public debate about a specific application of these types of orders because of their inherent secrecy.

Seizing this opportunity, my organization, Privacy International, has filed a case challenging the notices regime at the U.K.'s *The Investigatory Powers Tribunal*. Apple has filed a similar challenge.

Privacy International is devoting significant resources to opposing the Apple order because it exemplifies the potential for the notice regime to have far-reaching consequences that threaten our security and rights. That is because it appears that Apple has been ordered to deliberately weaken an end-to-end encrypted service.

We are concerned that this means that these notices now being used against encryption services in the U.K. will not stop with Apple.

My understanding from technical experts, including Professor Landau, is that it is technologically infeasible to have both effective end-to-end encryption and mechanisms for third-party access, which the U.K. seems to be demanding.

That is because to enable such third-party access creates an inherent vulnerability that can be exploited by bad actors, including hostile states and criminal networks.

That is why government security and privacy experts on both sides of the Atlantic, including in the U.S., the U.K., and the EU, strongly recommend using end-to-end encryption.

If the U.K. Government succeeds in maintaining this order against Apple, it is likely further such orders targeting end-to-end encryption may follow. Other American companies, given their global reach, will be targets.

Notices might also be used to force a company to do many other things that can undermine our security, such as sending false security updates or refraining from fixing a vulnerability in its systems.

Considering the notices regime's significant impact on fundamental rights and American companies, questions have been raised about the interaction of these orders with the CLOUD Act.

In some ways, the notices regime and the CLOUD Act operate independently of each other as the U.K. claims the ability to serve an order directly on a U.S. company, irrespective of the CLOUD Act.

The CLOUD Act itself steers clear of encryption with the Department of Justice declaring the act "encryption neutral."

Once a U.S. company is ordered to create a back door in its end-to-end encrypted services, the U.K. could then serve a production order on that company for information that would have been previously inaccessible, tying the notices regime and the CLOUD Act back together.

These secret orders also significantly impact fundamental rights, such as privacy and freedom of speech, and the CLOUD Act was intended to protect these rights, as well as U.S. companies.

The only other country with a CLOUD Act data access agreement, Australia, also has a Technical Capability Notices regime. The European Union, which is negotiating a data access agreement, has been considering measures that would undermine end-to-end encryption.

More countries therefore might soon be targeting U.S. companies and undermining the security and privacy of their users worldwide while also taking advantage of CLOUD Act processes. This clearly raises the question of whether the CLOUD Act encryption neutrality is truly sustainable, which I suspect my fellow panelists are now eager to answer.

Thank you.

[The prepared statement of Ms. Wilson Palow follows:]

Foreign Influence on Americans' Data Through the CLOUD Act

Before the Subcommittee on Crime and Federal Government Surveillance
of the Committee on the Judiciary

June 5, 2025

Testimony of
Caroline Wilson Palow, Legal Director and General Counsel,
Privacy International

On behalf of Privacy International (PI), thank you for the opportunity to testify about the impact of foreign surveillance powers, particularly those of the United Kingdom, on Americans' data and the CLOUD Act. Privacy International is a nonpartisan, U.K.-based charity that advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. PI has an office in London and is funded by foundation grants and individual donations.[1]

In this statement, I describe a troubling surveillance power that allows the U.K. Government to secretly order a U.S. company to undermine the security and privacy of its users worldwide. That power is enshrined in the U.K.'s Technical Capability Notice (TCN) regime, which I will detail here, along with how that regime purportedly has been applied to Apple, concerns about the wisdom and legality of the Apple TCN, and how the TCN regime and other countries' similar powers interact with the CLOUD Act. The current state of play threatens the privacy and security of Americans, and indeed people worldwide, by undermining the crucial protection of encryption.

[1] Details of PI's financials: https://privacyinternational.org/about/financials

The U.K.'s Technical Capability Notice Regime

The surveillance power at the core of today's discussion is the U.K.'s ability to serve a Technical Capability Notice (TCN) on a relevant operator, including companies providing telecommunications services, as enumerated in the U.K. Investigatory Powers Act 2016 (IPA). The following are the main components of the TCN regime:

What is a TCN? TCNs are orders, issued by the U.K. Government, which can be used to force operators to architect their systems to comply with other relevant surveillance authorizations under the IPA,[2] such as warrants authorizing interception[3] or hacking, authorizations for the collection of metadata, or bulk warrants that permit untargeted use of these powers. TCNs may require, *inter alia*, "the removal by a relevant operator of *electronic protection* applied by or on behalf of that operator to any communications or data" (emphasis added) or matters "relating to the security" of a system.[4]

Who can receive a TCN? A TCN can be given by a U.K. Secretary of State, often the Home Secretary, to a "relevant operator," which includes a postal or telecommunications operator. Most germane here, telecommunications operators are defined as those who offer, provide or control telecommunications services used by people in the U.K. Telecommunications services are broadly defined and can include phone and internet communications.[5]

What is the extraterritorial reach of a TCN? The definition of a relevant operator is broad enough to encompass service providers that are not based in the U.K., but merely offer services which are used in the U.K. This is made explicit in IPA section 253(8), which states a TCN "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside of the United Kingdom)." The U.K. thus claims the ability to serve TCNs on U.S.-based companies, among others. The U.K. Government recently doubled down on the extraterritorial application of TCNs by expanding the definition of the operators on which they could be served so as to "continue to apply to the operators to whom it was intended to apply, including those that have adopted more complex corporate structures."[6] This enhanced

---

[2] Investigatory Powers Act 2016 (hereinafter "IPA"), §253 (Eng.).
[3] Interception, as understood in the U.K., is broader than the American concept. U.K. interception warrants can authorize live wiretaps, such as permitted under the U.S. Wiretap Act, or access to stored communications, which would be authorized in the U.S. under the Stored Communications Act.
[4] IPA, §253(5).
[5] IPA, §261.
[6] *See* Investigatory Powers Act 2016 Consultation: Revised Notices Regime, June 2023, Objective 3, at 11:

definition became part of the Investigatory Powers (Amendment) Act 2024 (IPAA), which expands "telecommunications operators" to include those who control or provide a telecommunications system which is "used by another person to offer or provide telecommunications service to persons in the United Kingdom."[7]

What is the process for serving and challenging a TCN? The U.K.'s Secretary of State initiates the process of giving a TCN to an operator.[8] If the Secretary is considering serving a TCN, she must first consult with the operator who may be served and consider, among other things, the cost and feasibility of compliance.[9] Once the Secretary decides to serve the TCN, it must be approved by a Judicial Commissioner.[10] TCNs must be necessary and proportionate to their aim, as well as practicable to impose and comply with.[11] Once issued, the TCN is enforceable by injunction against operators inside and outside of the U.K.[12] Operators subject to a TCN may pursue an internal appeal, of sorts, by referring the TCN back to the Secretary for a second look, which includes consultation with a Technical Advisory Board, and approval by the head of the U.K. independent oversight body, the Investigatory Powers Commissioner.[13] In a change included in last year's IPAA, although not yet in effect, the operator must freeze any systems implicated by the TCN during this referral period, to avoid making "a change that, if implemented, would have a negative effect on the capability of the person to provide any assistance which the person may be required to provide in relation to any warrant, authorisation or notice issued or given under this Act."[14]

If a notice is upheld after referral, the process for challenging a TCN is less clear, although the Investigatory Powers Tribunal, a UK tribunal which hears challenges to the UK's investigatory powers and the actions of its intelligence agencies, has authority to provide redress to anyone who believes they have been the victim of unlawful action

---

https://assets.publishing.service.gov.uk/media/6475e2c0b32b9e000ca95e74/Revised_notices_regimes_consultation.pdf

[7] IPA, §261(10)(c).

[8] IPA, §253(1).

[9] IPA, §§255(2)-(4).

[10] IPA, §254. A Judicial Commissioner is a serving or retired senior judge who supports "the Investigatory Powers Commissioner in his oversight duties by providing independent authorisation of applications for the use of certain investigatory powers." Investigatory Powers Commissioner's Office, *Judicial Commissioners* (accessed June 2, 2025), at https://www.ipco.org.uk/who-we-are/judicial-commissioners/

[11] IPA, §253(1), (4).

[12] IPA, §255(10).

[13] IPA, §257.

[14] IPA §257(3B), once it comes into effect.

by a public authority using covert investigative techniques, including specifically TCNs.[15]

Are TCNs secret? An operator who receives a TCN "must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."[16] Thus, an American company subject to a TCN cannot reveal even its existence to U.S. officials and oversight bodies, much less external security experts, non-profit organizations, or users who play crucial roles in vetting the legality and wisdom of such Notices, which can have profound effects on all of our security and privacy. The Secretary of State has the power to allow an operator to discuss a TCN or its provisions.[17]

Recent changes to the TCN regime. As noted throughout this section, in 2024 the U.K. amended the IPA to add certain provisions expanding the reach of TCNs. In addition to the changes already mentioned, the U.K. created a new form of notice called a "Notification Notice."[18] While the Notification Notice provisions have not yet come into effect, they will have serious consequences when they do. A Notification Notice, if served on an operator, would require that operator to notify the U.K. Home Secretary if it plans to make a "relevant change" to its systems. A relevant change is defined extremely broadly, with the clear intent of requiring subject companies to notify the Home Secretary if they plan to implement any privacy and security measures that could affect their ability to comply with any other surveillance requirements under the IPA.

The new power appears to be squarely aimed at innovations and updates to encryption technology as well as other security features.[19] In relation to the latter, during the legislative debates surrounding the Act, the U.K. Government denied that security patches could be subject to the notification requirement. It did not rule out that Notification Notices could be used to gather this information, however, stating instead that: "we cannot foresee a circumstance in which a security patch would have

---

[15] Regulation of Investigatory Powers Act 2000 (hereinafter "RIPA"), §65(5)(czi) (Eng.).
[16] IPA, §255(8).
[17] *Id.; see also* Interception of Communications Code of Practice, Dec. 2022, §§ 8.23-8.25 (Eng.), at https://assets.publishing.service.gov.uk/media/639879928fa8f5530be3004b/revised_Interception_of_Communications_Code_of_Practice_Dec_2022.pdf (detailing potential scenarios in which the Secretary of State may consider allowing the operator to discuss a TCN with external people or institutions).
[18] Investigatory Powers (Amendment) Act 2024 (hereinafter "IPAA"), §21 (Eng.), to become IPA, §258A.
[19] *See* Draft Statutory Instrument on The Investigatory Powers (Codes of Practice, Review of Notices and Technical Advisory Board) Regulations 2025, §3, available at https://www.legislation.gov.uk/ukdsi/2025/9780348270716/introduction (defining a "relevant change" for the purpose of notification as, *inter alia*, "a change in the relevant operators ability to lawfully provide the content of communications", but not including a change that "fixes a defect in installed software and leaves the intended functionality of the software unchanged").

such a sweeping effect on lawful access capabilities." Should such a circumstance come to pass, it is unclear whether the U.K. would exercise its unfettered power. Like TCNs, Notification Notices are served in secret with companies prevented from revealing their existence. They also lack the crucial safeguard of being approved by a Judicial Commissioner.

As the foregoing demonstrates, the TCN regime gives the U.K. Government the power to attempt to alter the systems of companies the world over, so long as they have even a tenuous connection to providing telecommunications services in the U.K. That power is effectively unlimited in its scope, potentially requiring the re-architecture of critical infrastructure that provides privacy and security for all of us.

The Apple TCN

On February 7, 2025, the Washington Post reported[20] that the U.K. Home Secretary had served Apple with a TCN. The TCN purportedly targets Apple's Advanced Data Protection (ADP) service, which is an optional security feature for Apple users providing end-to-end encrypted (E2EE) iCloud storage which only the Apple user, and not Apple itself, can unlock. More specifically, an Apple user who turns on ADP secures their iCloud data using keys controlled by the user, not Apple. The TCN reportedly has worldwide effect, requiring Apple to undermine the security of ADP for all its users, not just those in the U.K.

Apple has neither confirmed nor denied the existence of the TCN. On February 21, 2025, however, Apple announced that it would be withdrawing its ADP services for UK-based Apple users.[21] The service is no longer available to new users in the U.K. and existing users expect the ADP functionality to be withdrawn soon. It seems reasonable to deduce from this withdrawal that Apple has received a TCN targeting ADP.

Apple then reportedly initiated a challenge to the TCN before the IPT,[22] which as mentioned above, hears legal claims against certain UK surveillance powers including TCNs. But the shroud of secrecy continued, as Apple did not admit to its challenge, nor did the U.K. government. The IPT listed a closed hearing without identifying the

---

[20] Joseph Menn, *U.K. orders Apple to let it spy on users' encrypted accounts*, Wash. Post, Feb. 7, 2025, at: https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/

[21] Zoe Kleinman, *Apple pulls data protection tool after UK government security row*, N.Y. Times, Feb. 21, 2025, at: https://www.bbc.co.uk/news/articles/cgj54eq4vejo

[22] Tim Bradshaw and Lucy Fisher, *Apple launches legal challenge to UK 'back door' order*, Fin. Times, Mar. 4, 2025, at: https://www.ft.com/content/3d8fe709-f17a-44a6-97ae-f1bbe6d0dccd

parties to the case.[23] This attracted much attention with multiple calls to open the hearing from media organizations, non-profit organisations, including PI, and a bipartisan group of members of Congress.[24]

Our collective suspicions were later confirmed when, on April 7, 2025, the IPT issued a judgment identifying Apple as the claimant that "filed a claim and a complaint in the Investigatory Powers Tribunal ("the Tribunal") raising issues as to the Secretary of State's powers to make Technical Capability Notices under the Investigatory Powers Act 2016."[25] The IPT's judgment is carefully worded in that it refers only to a generic challenge to "powers to make" TCNs and does not admit any further details about the purported TCN. It leaves open the possibility, however, that more details may be forthcoming as the challenge progresses.

The Washington Post's reporting, and the significant press follow-up, have provided us with the potentially unique opportunity to have a public debate about a specific application of a TCN because, as noted above, under the current state of the law, targets of TCNs themselves cannot reveal them.

Seizing that opportunity, the day before the IPT's closed hearing on Apple's challenge, PI and three co-claimants filed a public challenge to the TCN regime. PI's co-claimants are Liberty, another charity that defends fundamental human rights and freedoms in the U.K., and two individuals, PI Executive Director Gus Hosein and the director of the American Civil Liberties Union's Speech, Privacy, and Technology Project, Ben Wizner.

PI's complaint questions the legality of the TCN served on Apple as well as the TCN regime in general, alleging that the Apple TCN is ultra vires, disproportionate and lacks sufficient safeguards to be in accordance with the law. The IPT allows cases to proceed on hypothetical facts, which means neither Apple nor the U.K. Government need to admit the details of the TCN for PI's challenge to proceed. In its April 7th judgment, the IPT suggested PI's case may go forward in parallel with Apple's or proceed while Apple's is stayed.[26]

---

[23] Bill Goodwin, *Secret London tribunal to hear appeal in Apple vs government battle over encryption*, Computer Weekly, Mar. 11, 2025, at: https://www.computerweekly.com/news/366620363/Secret-London-tribunal-to-hear-appeal-in-Apple-vs-government-battle-over-encryption

[24] *See* Apple Inc v. Secretary of State for the Home Office (2025) UKIPTrib 1, available at: https://investigatorypowerstribunal.org.uk/judgement/apple-inc-v-secretary-of-state-for-the-home-department/

[25] *Id.*

[26] *Id.*

As of the date of this testimony, PI and its co-claimants have filed expert witness evidence with the IPT and are awaiting the U.K. Government's response to their complaint. The potential for further submissions in both PI's case and Apple's is still being considered by the IPT.

Security and Privacy Consequences of the Apple TCN

The Apple TCN exemplifies the potential for the TCN regime to have far reaching consequences that threaten our security and rights. It appears that Apple has been ordered to deliberately weaken ADP, which is an end-to-end encrypted (E2EE) service. E2EE is a fundamental security protection. It also plays an essential role in the protection of privacy, free expression, and freedom of association. Weakening E2EE can have a profound effect on our personal and professional lives.

Encryption plays a critical role in data privacy and security by safeguarding online communications and data, enabling free speech, and providing protection for financial and legal transactions, amongst other things. Indeed, encryption is often mandatory from a regulatory perspective for organisations in areas such as healthcare, education, finance and banking.

What distinguishes E2EE from other encryption methods is that the data is encrypted before it is transmitted from a user's device and decrypted only after reaching its intended destination. As the encryption and decryption of data sent and received occurs on users' devices, E2EE provides only the intended recipients – not even the communications service or data storage provider – with access to the content of the message. E2EE ensures that third parties, including the service providers themselves, cannot decrypt the data being transmitted or stored, as the decryption keys are not accessible to them. The provider of storage or communication services is not trusted with access to the data, not least because there is a risk of compromise, hacking or improper use by or through the provider's services.

Such issues are not hypothetical. By way of example, in August 2022, the New York Times reported that a Twitter employee was convicted of spying for Saudi Arabia.[27] The individual allegedly used his access at Twitter to gathered personal information of political dissidents to pass to Saudi Arabia for payment. Service providers may also be

[27] Kalley Huang and Kate Gonger, Former Twitter Employee Convicted of Charges Related to Spying for Saudis, N.Y. Times, Aug. 9, 2022, available at: https://www.nytimes.com/2022/08/09/technology/twitter-saudi-arabia-spying-ahmad-abouammo.html

the subject of hacking and data breaches, or legal proceedings initiated in states that do not respect fundamental rights.

My understanding is that ADP operates using E2EE. Under ADP, Apple does not have access to the keys needed to decrypt data covered by ADP (which is stored in encrypted form on its servers and while being transmitted over the internet). It is therefore impossible for Apple to access any such data. Once ADP is enabled, the user takes control of the key, providing end-to-end security for the data. Without ADP enabled, Apple retains the key used to encrypt the cloud storage. As Apple holds the key in this scenario, it can be compelled to disclose that key or the information protected by it, and that information is vulnerable to hacking of Apple's systems by bad actors.

As we do not know the details of the Apple TCN, we do not know if the U.K. Government is demanding Apple turn off ADP or asking for some form of "backdoor" allowing ADP to appear to remain available but with a way for the U.K. Government to gain access to the information it protects. Either way, using legal authority to undermine the security of E2EE has profound implications.

My understanding from technical experts, including one of my fellow panellists, is that it is technologically infeasible to have both effective E2EE and mechanisms for third-party access.[28] That is because the basis of E2EE's effectiveness is that only endpoint users can access the protected data. To enable anyone else's access creates an inherent vulnerability that can be exploited by bad actors, including both hostile states and non-state actors, such as criminal networks.

The U.K. Government has defended its TCN power by declaring that it would only facilitate the U.K.'s lawful access that is accompanied by robust, rights-protective safeguards. PI may disagree that the U.K.'s safeguards are as robust as claimed, but that is beside the point because our concern about TCNs is that once a backdoor is created, states with far less stellar records on human rights, such as Russia and China, could seek similar access through legal process. Or exploit the vulnerability created without following legal process. Either way, by demanding third-party access to data, files and other content protected by E2EE, governments interfere with strong encryption and necessarily make our increasingly digital societies less secure.

---

[28] *See, e.g.*, PI, *Securing Privacy: Privacy International on End-to-End Encryption*, at https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption; Abelson H., et al., *Keys Under Doormats: Communications of the ACM* (2015).

This insecurity could affect the billions of people who daily use E2EE services. For example, WhatsApp, iMessage and Signal are popular E2EE messaging services. WhatsApp alone has three billion users.[29]

Governments also promote the use of end-to-end encryption. The Federal Cyber Defense Skilling Academy (CISA) provides public guidance that "highly targeted individuals", such as those in senior government or political positions, should "use only end-to-end encrypted communications."[30] Prior to the Apple TCN becoming public, the U.K. National Cyber Security Centre (NCSC) encouraged barristers and solicitors to use E2EE services, including ADP.[31] The European Data Protection Board (EDPB) and European Data Protection Supervisor (EDPS) agree, opining that "end-to-end encryption ('E2EE') is a crucial tool for ensuring the confidentiality of electronic communications, as it provides strong technical safeguards against access to the content of the communications by anyone other than the sender and the recipient(s), including by the provider."[32]

As Professor Ciaran Martin (formerly head of the U.K.'s NCSC which is part of the Government Communications Headquarters (GCHQ)[33]) has put it, the reality is that senior politicians and officials use, and need to use, ordinary and widely available E2EE products that are not subject to government-mandated backdoors: "these friends and colleagues are acting rationally, not hypocritically: their important work can, sometimes, be better protected in this way. That's why this revolution in digital security cannot, Canute-like, be wished away, any more than public key cryptography could be held back indefinitely… It is now a national and international imperative that our increasingly digital societies are increasingly digitally secure."[34]

---

[29] *See* Laura Ceci, *Number of monthly active WhatsApp users worldwide from April 2013 to March 2025*, Statista, May 5, 2025, at https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

[30] Cybersecurity and Infrastructure Security Agency (CISA), Mobile Communications Best Practice Guide, Dec. 18, 2024, at https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

[31] National Cyber Security Centre, *Cyber security tips for barristers, solicitors and legal professionals*, originally at https://www.ncsc.gov.uk/files/Cyber-security-tips-for-barristers.pdf , archived by the WayBackMachine, at https://web.archive.org/web/20241102140713/https://www.ncsc.gov.uk/files/Cyber-security-tips-for-barristers.pdf (accessed June 2, 2025).

[32] EDPB-EDPS, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, § 97 (adopted July 8, 2022), at https://edpb.europa.eu/system/files/202207/edpb_edps_jointopinion_202204_csam_en_0.pdf

[33] GCHQ is the U.K's intelligence, security and cyber agency, which is roughly equivalent to the U.S. National Security Agency (NSA).

[34] Ciaran Martin, *End-to-End Encryption: the (Fruitless?) Search for a Compromise*,

Everyone benefits from having a private sphere in which to communicate and develop our opinions and beliefs, as well as to enable economic activity.[35] Some people may have heightened duties of confidentiality or be at increased risk of unlawful surveillance, making the protections of E2EE essential. These people include law enforcement and government officials, journalists, researchers, lawyers, non-profits, activists, human rights defenders, marginalised and vulnerable groups.[36] The UN High Commissioner for Human Rights has highlighted the privacy risks posed by measures that undermine encryption and recommends that governments "avoid all direct, or indirect, general and indiscriminate restrictions on the use of encryption, such as prohibitions, criminalization, the imposition of weak encryption standards or requirements for mandatory general client-side scanning."[37]

If the U.K. Government succeeds in maintaining this TCN against Apple, it is likely further TCNs targeting E2EE may follow. The U.K. Government has a long-held and recurring ambition to undermine E2EE.[38] For instance, such TCNs could be used to force Meta or Apple to remove or undermine the E2EE of WhatsApp and iMessage, respectively.[39]

E2EE is not the only security protection at risk, however. TCNs might also be used to force a company to send false security updates to its users, or to refrain from fixing a vulnerability in its systems. The TCN power is ill-defined. The IPA includes a list of five potential obligations that may be specified in a TCN, including those relating to: (1) providing facilities or services, (2) an apparatus owned or operated by the target

---

Blavatnik School of Government, University of Oxford, Nov. 23, 2021, at 11, available at https://www.bsg.ox.ac.uk/research/publications/end-end-encryption-fruitless-search-compromise

[35] *See, e.g.*, Article 29 Data Protection Working Party, Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11 April 2018), https://ec.europa.eu/newsroom/article29/items/622229/en ; Report of the United Nations High Commissioner for Human Rights on the Right to Privacy in the Digital Age, UN Doc A/HRC/39/29, § 21 (4 August 2022)

[36] PI, *Securing Privacy: Privacy International on End-to-End Encryption*, at https://privacyinternational.org/report/4949/securing-privacy-end-end-encryption

[37] *Report of the UN High Commissioner for Human Rights on the right to privacy in the digital age*, Aug. 4, 2022, UN Doc A/HRC/51/17, para 57(b).

[38] *See, e.g.*, PI, *Defeating encryption: the battle of governments against their people* , Feb. 1 2017, at https://privacyinternational.org/blog/674/defeating-encryption-battle-governments-against-their-people; PI, *Ghosts in Your Machine: Spooks Want Secret Access to Encrypted Messages,* May 29, 2019, at https://privacyinternational.org/news- analysis/3002/ghosts-your-machine-spooks-want-secret-access-encrypted-messages; PI, *No, the UK Hasn't Just Signed a Treaty Meaning the End of End-to-End Encryption*, Oct. 1, 2019, at https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption; Joe Mullin, *The U.K. Paid $724,000 For A Creepy Campaign To Convince People That Encryption is Bad. It Won't Work*, EFF, Jan. 21, 2022, at https://www.eff.org/el/deeplinks/2022/01/uk-paid-724000-creepy-campaign-convince-people-encryption-bad-it-wont-work.

[39] *See* IPA, §253(5)(c) (explicitly permitting TCNs relating to the removal of "electronic protection").

operator, (3) the removal of "electronic protection applied by or on behalf of" the operator, (4) the security of a postal or telecommunication service, or (5) the handling or disclosure of any information.[40] But that list is non-exhaustive. In theory, the U.K. Government could issue a TCN for any action the Home Secretary considers "necessary for securing that the operator or another relevant operator has the capability to provide any assistance" in carrying out interception, hacking or acquisition of metadata as permitted under the IPA, so long as that requirement is "practicable" for the operator.[41]

The Apple TCN is thus not only a threat to the security of Apple's services, but to E2EE in general, and potentially, if the TCN regime continues to exist in its current form, to the security of telecommunications services worldwide.

Legality of TCNs

A TCN requiring the undermining of E2EE is not only bad policy, it also likely violates U.K. law. Indeed, the TCN regime is particularly problematic due to its lack of transparency, disproportionality, and extraterritorial reach.

Lack of Transparency. The Apple TCN remains officially secret because of the IPA's strict gagging provision, which states "[a] person to whom a relevant notice is given, or any person employed or engaged for the purposes of that person's business, must not disclose the existence or contents of the notice to any other person without the permission of the Secretary of State."[42]

The gagging provision is legally problematic when combined with the ill-defined nature of the TCN power, as discussed above. That broad power fails to provide the necessary accessibility and foreseeability required of surveillance powers by U.K. law.[43] It is hard to see how a TCN that is entirely secret, and based on an ill-defined power, could be considered reasonably accessible and foreseeable to those it most affects,

---

[40] IPA, §§253(5)(a)-(e); *see also* The Investigatory Powers (Technical Capability) Regulations 2018, 2018 No. 253, available at https://www.legislation.gov.uk/uksi/2018/353/made (describing, in more detail, obligations the Secretary of State has declared to be practicable to impose).

[41] IPA, §§253(1)(a), (4).

[42] IPA, §255(8).

[43] Under Article 8(2) of the European Convention on Human Rights (ECHR), which is incorporated into U.K law by the Human Rights Act 1998, an interference with Article 8 rights is permitted only if it is "*in accordance with the law*" and "*necessary in a democratic society*" to achieve one or more of the aims specified in Article 8(2). An interference is "*in accordance with the law*" if it is lawful under domestic law and "*compatible with the rule of law*", i.e. "*accessible to the person concerned and foreseeable as to its effects.*" *Podchasov v. Russia*, Application No. 33696/19 (European Court of Human Rights), Feb. 13, 2024, at 61.

which are the users of the service targeted. There is no way of knowing the nature of any TCN, when or in what circumstances it might be made, or how long it will be in force. This total secrecy also precludes other important safeguards that protect against arbitrary conduct, such as notification of those affected by the TCN after it is terminated.

The gag further frustrates a legitimate and robust policy debate about the use of this highly intrusive power – a debate we are only now able to have due to the luck of having an intrepid reporter at the Washington Post. It also means American companies like Apple are not able to reveal and discuss TCNs with Congress or other oversight bodies.

Disproportionality. In the U.K., a surveillance power is unlawful if it is disproportionate to its legitimate aim. That means, even if it is used to pursue a legitimate goal, such as targeted law enforcement investigations, it may still not be lawful if the harm it causes to security, privacy and other rights outweighs that benefit. Applying this to the context of E2EE, the European Court of Human Rights[44] has recognised that a statutory obligation to decrypt E2EE communications "risks amounting to a requirement that providers of such services weaken the encryption mechanism for all users" and thus is "not proportionate."[45] It went on to conclude that measures that "permit authorities to have access, on a generalised basis and without sufficient safeguards, to the content of electronic communications…" will necessarily impair "the very essence of the right to respect for private life."[46]

As an initial matter, because the Apple TCN has not been disclosed, we do not know if its purpose is legitimate. The U.K. Government is firmly maintaining its neither confirm nor deny position on the TCN, so has not revealed its whether it is to assist law enforcement or protect national security, much less a justification for why it should remain secret.

Even if the TCN has a legitimate aim, however, it is disproportionate. The reported TCN is blanket and indiscriminate in nature, affecting all of Apple's ADP functionality worldwide. There is no requirement that the relevant persons have been engaged in any wrongdoing or criminality: it is enough that they own an Apple device. This not only deeply impacts Apple users' privacy rights (as well as the rights of any other persons whose data is being stored by users on iCloud), but also their freedom of

[44] As a Council of Europe member-state, the U.K. abides by the European Convention on Human Rights, which is subject to the judicial supervision of the European Court of Human Rights. The Convention guarantees, among others, the right to privacy.
[45] *Podchasov*, Application No. 33696/19 at 79.
[46] *Id.* at 80.

expression. E2EE plays an essential role in enabling and facilitating free speech. It is invaluable to vulnerable groups, including minorities, journalists and political opponents (among others). And, as discussed in detail above, requiring a backdoor in ADP creates a vulnerability that puts the security of all users at risk from rogue nation states and criminals alike. Breaking E2EE in these circumstances is not justifiable.

Ultimately, the privacy and security implications of TCNs are profound because, as discussed above, a TCN can demand systemic change. That is, using a TCN, the U.K. Government can demand that operators alter their services in a way that may deeply affect all users. That cannot be proportionate.

Extraterritorial Reach. IPA section 253(8) states a TCN "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside of the United Kingdom)." This is bolstered by the definition of a relevant operator, which is broad enough to encompass service providers who are not based in the U.K., but merely offer services which are used in the U.K.

While the extraterritoriality of TCNs is not clearly a violation of U.K. law, it could result in targets of TCNs being faced with potential conflicts of laws. For instance, a European company may find itself struggling to comply with data protection obligations if a TCN requires it to undermine the security of its systems and not tell its users about that change. An American company might similarly be placed in the position of being forced to lie about the security of its products, a misrepresentation or omission which could be considered a deceptive trade practice. Undermining E2EE also squarely conflicts with American public policy such as the CISA's promotion of encryption as a strong security measure.[47]

TCNs and the CLOUD Act

Considering the TCN regime's significant impact on fundamental rights and American companies, several questions have been raised about the interaction of TCNs and the CLOUD Act. I address my understanding of that interaction in this section.

In some ways, the TCN regime and the CLOUD Act operate independently of each other.[48] As described above, the IPA includes exterritorial enforcement provisions that

[47] Cybersecurity and Infrastructure Security Agency (CISA), Mobile Communications Best Practice Guide, Dec. 18, 2024, at https://www.cisa.gov/sites/default/files/2024-12/guidance-mobile-communications-best-practices.pdf

[48] *See, e.g.*, PI, *No, the UK Hasn't Just Signed a Treaty Meaning the End of End-to-End Encryption*, Oct. 1, 2019, at https://privacyinternational.org/news-analysis/3242/no-uk-hasnt-just-signed-treaty-meaning-end-end-end-encryption

do not rely on the CLOUD Act. Thus, the U.K. claims the ability to serve a TCN directly on a U.S. company irrespective of the CLOUD Act.

The existence of the TCN regime and its potential impact on encryption, however, were raised by PI and others while the CLOUD Act was being drafted.[49] Despite these concerns, the CLOUD Act steers clear of encryption, touching on it only when requiring that Executive Agreements "not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data."[50] At the time of the signing of the U.K Executive Agreement, the Department of Justice (DOJ) declared the CLOUD Act "encryption neutral". According to the DOJ, "[t]his neutrality allows for the encryption issue to be discussed separately among governments, companies, and other stakeholders."[51]

Yet TCNs may have significant effects on fundamental rights and American companies. We raised TCNs during the CLOUD Act negotiation because they are a core component of U.K. surveillance law. The goal of the CLOUD Act, as evidenced by its Congressional Findings, was to minimize conflicts of laws while preserving the "protection of privacy and civil liberties."[52] Allowing TCNs to be served on American companies creates a potential conflict of laws, as noted above, and severely infringes privacy and civil liberties.

Other provisions of the CLOUD Act are also implicated by the TCN regime. To enter into an Executive Agreement, a foreign government's domestic law must be assessed as to a number of factors.[53] Several of those factors require adherence to international human rights standards, including protection from arbitrary and unlawful interference with privacy and freedom of expression. Another factor demands the foreign government have "sufficient mechanisms to provide accountability and appropriate transparency regarding the collection and use of electronic data."[54] The TCN regime, especially as applied in the case of the Apple TCN, fails to satisfy any of these factors because, as alleged in our challenge and detailed above, (1) it is disproportionate and lacks the necessary qualities of accessibility and foreseeability, leading to an

---

[49] *See, e.g.*, Center for Democracy and Technology, *Cross-Border Law Enforcement Demands: Analysis of the US Department of Justice's Proposed Bill*, Aug. 17, 2016, at https://cdt.org/wp-content/uploads/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf

[50] Electronic Communications Privacy Act of 1986 (hereinafter "ECPA"), 18 U.S.C. §2523(b)(3).

[51] U.S. Dep't of Just., Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act, April 2019, at 6, at https://www.justice.gov/archives/opa/press-release/file/1153446/dl?inline=

[52] CLOUD Act, Public L. No. 115-141, §102(6) (2018).

[53] ECPA, 18 U.S.C. §2523(b)(1)(B).

[54] *Id.* §2523(b)(1)(B)(v).

infringement of privacy and free expression, and (2) operates in complete secrecy, lacking all transparency.

Finally, once in place, the Apple TCN could open all iCloud data to U.K. Government access via the CLOUD Act. Once a backdoor is created in ADP, the U.K. could serve an overseas production order on Apple under the CLOUD Act seeking access to data protected by ADP. So long as the production order does not violate any of the CLOUD Act provisions, such as the prohibition on seeking data belonging to U.S. persons, then Apple would have few grounds on which to refuse to use the backdoor to access the requested data.

The only other country with an Executive Agreement, Australia, also has a Technical Capability Notice regime.[55] Australia's TCNs appear to be more narrowly defined than the U.K.'s in that the Australian Government asserts "nothing in this legislation can require industry to break encryption."[56] There is some debate, however, as to whether Australian TCNs may still raise security concerns or even permit access to E2EE data in a more targeted way.[57]

Furthermore, the European Union (EU) is negotiating an Executive Agreement.[58] While I am not aware of any EU country having a TCN-like regime, several countries and the EU itself have recently been considering measures that would undermine E2EE.[59]

---

[55] Austl. Gov't Dep't of Home Affairs, The Assistance and Access Act 2018, Jun. 5, 2023, at https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-encryption

[56] *Id.*

[57] *See, e.g.*, Peter Alexander Earls Davis, *Decrypting Australia's 'Anti-Encryption' legislation: The meaning and effect of the 'systemic weakness' limitation*, Computer Law & Security Review, Vol. 44 (April 2022), at https://www.sciencedirect.com/science/article/pii/S0267364922000073

[58] U.S. Dep't of Just., *Justice Department and European Commission Announces Resumption of U.S. and EU Negotiations on Electronic Evidence in Criminal Investigations*, Mar. 2, 2023, at https://www.justice.gov/archives/opa/pr/justice-department-and-european-commission-announces-resumption-us-and-eu-negotiations

[59] Sweden is currently considering legislation that could compromise encryption, *see* Global Encryption Coalition, Joint Letter on Swedish Data Storage and Access to Electronic Information Legislation, Apr. 8, 2025, at https://www.globalencryption.org/2025/04/joint-letter-on-swedish-data-storage-and-access-to-electronic-information-legislation/; France recently rejected a similar measure, *see* Electronic Frontier Foundation, A Win for Encryption: France Rejects Backdoor Mandate, Mar. 21, 2025, at https://www.eff.org/deeplinks/2025/03/win-encryption-france-rejects-backdoor-mandate; and the EU has been debating a regulation that would require scanning of E2EE communications, among other things, *see, e.g.*, Global Encryption Coalition, GEC Steering Committee Statement on 9 September Text of the European CSA Regulation, Sept. 16, 2024, at https://www.globalencryption.org/2024/09/gec-steering-committee-statement-on-9-september-text-of-the-european-csa-regulation/.

In light of the interactions between the TCN regime and the CLOUD Act, as well the existence of surveillance regimes in other countries currently in or negotiating Executive Agreements, effective protection of our security and rights may require consideration of whether the CLOUD Act's purported encryption neutrality is sustainable.

Mr. TIFFANY. [Presiding.] Thank you, Ms. Wilson Palow. Now, I'd like to turn to Mr. Salgado.

You have five minutes for your testimony.

STATEMENT OF RICHARD SALGADO

Mr. SALGADO. Thank you, Mr. Congressman. Thank you, Chair Biggs, Ranking Member McBath, Chair Jordan, and Ranking Member Raskin, for inviting me here today to participate in this hearing on these important issues and for your leadership on this.

My name is Richard Salgado. The Chair summarized my more than 35 years of experience as a lawyer, mostly dealing with government surveillance and network security issues.

It was almost exactly eight years ago that I testified about the need for changes that were ultimately included in the CLOUD Act and signed into law by President Trump in 2018. I'm honored to be here again now that we've gained some experience with the act and the agreement that the U.K. entered pursuant to it.

Even in these relatively early days, it's clear that the act provides a framework for advancing U.S. interests and public safety. It underscores the importance of finalizing agreements with Canada, the European Union, and beginning negotiations with other countries.

Deeply concerning is the report by *The Washington Post* in February that the U.K. is secretly seeking to compel Apple to disable a global security feature in one of its products to expand its surveillance capabilities. It also illustrates the value of the CLOUD Act framework.

When a foreign government coerces an American company to compromise or withhold security protections intended to safeguard users worldwide, the impact reaches everyone, including Americans. The harm is magnified when such mandates are imposed in closed, secret proceedings with outcomes concealed.

These actions threaten core U.S. interests in cybersecurity and erode the global competitiveness of American technology providers in the light of serious competition from China.

If there is still a real debate about whether security should yield to government surveillance, it doesn't belong behind closed doors in a foreign country. It shouldn't be settled in secret proceedings run by foreign officials and with outcomes unknown even to the U.S. Government.

The debate belongs in public, before the U.S. Congress, led by officials elected by the American people, acting with the interests of this country at heart. It must be decided here, not imposed there.

Regardless of the outcome in the reported Apple matter, which we may never know, this experience reflects the broader threat of foreign efforts to covertly undermine the security of products and services offered by American companies. We are now tasked with identifying and implementing solutions.

Fortunately, the CLOUD Act provides an ideal framework for this. The CLOUD Act provisions at issue today were enacted to address problems created by U.S. blocking statutes.

Before the act, U.S. providers were broadly and presumptively barred from disclosing certain user data to foreign governments,

even when the request came from a jurisdiction that respects human rights and the rule of law and in a legitimate case.

As a result, countries had to rely on diplomatic tools, like Mutual Legal Assistance Treaties, which are often too slow in practice. Frustrated, some would resort to unilateral measures to circumvent U.S. law, including tactics that undermine security.

The CLOUD Act addresses this by conditionally lifting the blocking statutes for any country that qualifies for and signs an Executive agreement with the U.S. To qualify, a government must demonstrate respect for civil liberties and due process, among other requirements.

Once an agreement is in place, a U.S. provider may honor data requests from that country without risking running afoul of the blocking statutes.

With a few surgical changes, the CLOUD Act is well-suited to address the U.K.'s reported actions and similar moves by other foreign governments. I have outlined several improvements in my written testimony and will briefly summarize only a few here.

First, the U.S. Government should press the U.K. to end its reported effort against Apple and commit to refraining from similar actions against other American companies. That commitment should be a condition for continued participation in the agreement.

Second, Congress should amend the CLOUD Act to declare cybersecurity a national interest that, like free speech, must be respected.

Third, Congress should require that to qualify for an agreement a foreign government must not impose surveillance or antisecurity obligations on American companies.

With these targeted changes and a few others, the act can better advance cybersecurity and help American companies continue offering trusted, secured services worldwide. We should treat the lamentable U.K. episode as a lesson and improve the act. Too much is at stake otherwise.

Thank you for the opportunity to discuss these issues.

[The prepared statement of Mr. Salgado follows:]

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

@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.

Mr. TIFFANY. Thank you, Mr. Salgado. Mr. Nojeim, you have five minutes for your testimony.

STATEMENT OF GREGORY T. NOJEIM

Mr. NOJEIM. Thank you so much, Acting Chair Tiffany, Ranking Member Raskin, and the Members of the Subcommittee.

My name is Greg Nojeim and I direct the Security and Surveillance Project at the Center for Democracy and Technology. I'm proud to say that our awesome intern class is here and showed up.

Thank you for identifying yourselves.

Mr. TIFFANY. Welcome.

Mr. NOJEIM. The CDT is a nonprofit, nonpartisan organization. As the Chair mentioned, we defend civil rights, civil liberties, and democratic values in the digital age.

We're calling on Congress to act with the DOJ to protect the privacy and security of Americans' data against threats from countries that benefit from CLOUD Act agreements.

Congress enacted the CLOUD Act in 2018 by tacking it onto the end of a 2,322-page omnibus spending bill. It empowers the DOJ to enter into Executive agreements without congressional approval with foreign countries through which the U.S. providers can disclose user data from storage and in real time. Disclosures are made directly to foreign states under the laws of the foreign State, and the U.S. warrant requirement that would otherwise pertain does not apply.

The U.K. has availed itself of this opportunity in spades, issuing over 20,000 demands under the CLOUD Act. In contrast, the U.S. has issued 63.

The benefits of the agreement to the U.S., while real, are limited. CLOUD Act agreements are supposed to preserve the privacy of Americans and of other people in the United States. The foreign country cannot target those people with CLOUD Act orders.

Things haven't quite worked out as Congress planned. Instead, the U.K. has ordered Apple, as the other witnesses have said, under the authority of U.K. law, not under the authority of the CLOUD Act, to build in a back door to its encrypted cloud backup service so Apple can fulfill the U.K.'s CLOUD Act demands.

If Apple had fully complied, it would have compromised the communications security of its users in the U.S. and worldwide.

The U.K. law, the TCNs, are super-extraterritorial. The U.K. authorities can issue orders on companies headquartered outside the U.K. and order them to alter their equipment that is outside the U.K. so they can wiretap people who are outside the U.K.

We don't know how many other U.S. providers have received one of these orders. If they have received one, they are gagged and can't say so.

Other countries assert authority to compel this type of provider assistance. Australia is the only other country to have a CLOUD Act agreement. If has a similar law similar to the U.K.'s, but it includes a vague exception that may protect encryption.

Canada, which is negotiating a CLOUD Act agreement with the U.S. right now, has a provision almost identical to the Australian law provision.

Acting Chair Tiffany, if you are an iPhone user and you go to London and you try to back up your iMessages with the cloud backup service that Apple provides, you wouldn't be able to do it in encrypted form. The reason you wouldn't be able to do it is because Apple has withdrawn that service from the U.K. under the pressure of this order that it's received.

The U.K. would have Apple withdraw the service worldwide or compromise its protections so that no matter where you went, even to your office next door in the Cannon Building, if you downloaded your iMessages you wouldn't be able to protect them with encryption.

This situation is intolerable. The DOJ and Congress should put an end to it by taking three steps.

First, the DOJ should invoke Article 12.3 of the agreement and declare that it is infective with respect to CLOUD Act orders issued to a provider that has received an order like the one served on Apple. Such a declaration would have an immediate effect.

The DOJ should also persuade the U.K. to publicly withdraw the order to Apple, under threat of terminating the agreement, unless the U.K. agrees. This has the benefit of a negotiated result with more predictable public effect that sends a message to other countries that seek CLOUD Act agreements.

Finally, Congress should back up the DOJ by amending the CLOUD Act to prohibit CLOUD Act agreements with countries whose laws or practices permit such orders and to require CLOUD Act agreements—that they explicitly prohibit such orders.

We look forward to working with you on such solutions.

[The prepared statement of Mr. Nojeim follows:]

Testimony of Gregory T. Nojeim

Director, Security and Surveillance Project

Center for Democracy & Technology

before the

House Judiciary Committee
Subcommittee on Crime and Federal Government Surveillance

On

"Foreign Influence on Americans' Data Through the CLOUD Act"

June 5, 2025

Chairman Biggs, Ranking Member McBath, and Members of the Subcommittee:

My name is Greg Nojeim, and I direct the Security and Surveillance Project at the Center for Democracy & Technology (CDT). CDT is a nonprofit, nonpartisan organization that defends civil rights, civil liberties, and democratic values in the digital age. For nearly three decades, CDT has worked to ensure that rapid technological advances promote democracy and human rights.

We are calling on Congress and the Department of Justice (DOJ) to protect the privacy and security of Americans' data against threats to it by countries that benefit from agreements entered into under the U.S. CLOUD Act. The first country to receive the benefits of a CLOUD Act agreement — the United Kingdom — has ordered Apple, a U.S. communication service provider, to build in a backdoor to its encrypted cloud back up service to facilitate surveillance demands the UK will make of Apple under the auspices of the CLOUD Act. Such a requirement compromises the privacy and security of the communications of everyone who uses that service even if they are not located in the United Kingdom, including Americans.

Today, I will:

- Explain why Congress enacted the CLOUD Act and describe the broad scope of the surveillance demands it authorizes, what the CLOUD Act omits, and how it fails to protect encryption;
- Indicate that CLOUD Act agreements entered into so far are silent on encryption, and explain how that silence has opened the door to problematic conduct by counties that benefit from CLOUD Act agreements;
- Show how the U.S. can and should use its leverage to protect encryption in the context of existing CLOUD Act agreements, and those into which it will enter in the future; and
- Outline changes Congress could make to the CLOUD Act to protect encryption if the Department of Justice (DOJ) does not act to do so.

How the CLOUD Act Facilitates Foreign Government Surveillance

Congress enacted the CLOUD Act in 2018 by tacking it on to the end of a 2,322-page omnibus spending bill. Reduced to its essence, the CLOUD Act did two things: (1) it granted U.S. law enforcement entities new powers to compel U.S. companies to disclose communications and data on U.S. and foreign users that is stored overseas when the U.S. companies can exercise control over that data, and (2) it empowered the DOJ to — without congressional approval — enter into executive agreements with foreign countries through which U.S. providers can disclose user data, from storage and in real time, directly to foreign states under the laws of those foreign states, subject to certain requirements.

We are focused on the latter change. It was accomplished by removing the block in the Electronic Communications Privacy Act that otherwise prohibited the direct disclosure of user content to a foreign governmental entity. Before the CLOUD Act, and today in the absence of a CLOUD Act agreement, the foreign government would have to make a request under the relevant Mutual Legal Assistance Treaty (MLAT) between the foreign government and the U.S., and enlist the DOJ to apply to a federal magistrate for a warrant, based on a showing of probable cause. The MLAT system is slow, and foreign law enforcement officials need speedy responses in order to investigate crimes in their own countries, and to prevent them. Moreover, MLAT agreements do not authorize foreign governments to engage in wiretapping by obtaining access to communications in real time. This real time access was particularly important to the UK, which lobbied Congress and elements of the U.S. government to include it in the CLOUD Act.

To preserve the privacy of Americans and of everyone in the U.S., the CLOUD Act requires that surveillance orders that a foreign government issues under a CLOUD Act agreement cannot intentionally target a U.S. person or a person located in the U.S. (18 U.S.C. § 2523(b)(4)(A-B)). In theory, they would remain protected under U.S. law and the U.S. Constitution, but, as explained later, their rights can still be compromised by the conduct of countries that enjoy the benefits of a CLOUD Act agreement. The CLOUD Act imposes other requirements, including limiting disclosures to cases involving serious crimes, and barring the DOJ from entering into a CLOUD Act agreement unless the DOJ can certify that the country's laws and practices meet certain human rights standards.

The CLOUD Act requires that "the terms of [CLOUD Act agreements] shall not create any obligation that providers be capable of decrypting data [...]," (18 U.S.C. § 2523(b)(3)). But the plain text of this provision does not prevent the U.S. from entering CLOUD Act agreements with countries that impose such obligations under domestic legal authorities, as long as the relevant CLOUD Act agreement does not directly impose those obligations. CDT opposed the CLOUD Act in part because it did not sufficiently safeguard encrypted services.

So far, the U.S. has entered into two CLOUD Act agreements: one with Australia, and one with the United Kingdom (UK).[1] The UK-U.S. CLOUD Act Agreement ("Agreement") entered into force on October 3, 2022. Under its terms, the Agreement expires after five years unless renewed by an exchange of diplomatic notes, which means it is set to expire on October 3, 2027. Notably, the Agreement is silent on encryption. But that silence speaks volumes: the CLOUD Act Agreement clears the way for the UK to make surveillance demands on U.S. providers under UK law, but does nothing to ensure that the UK cannot require U.S. providers to decrypt otherwise encrypted communications and thereby compromise users' privacy and security.

[1] Negotiations have been initiated with at least two other foreign governments: Canada and the European Union. It is not apparent whether these negotiations are ongoing.

The UK Has Ordered Apple To Compromise Cybersecurity Worldwide

The UK's Investigatory Powers Act (IPA) of 2016, commonly known as the "Snoopers' Charter," grants sweeping surveillance authorities, including the ability to issue Technical Capability Notices (TCNs) to communication service providers. Under this provision, the UK Home Office can compel providers to make changes to their systems and services to ensure they have the ability to give effect to surveillance demands. This includes requirements to remove electronic protections like end-to-end encryption. Crucially, TCNs can be issued secretly, and can gag the provider who receives the order from disclosing its existence even to authorities in its home country. TCNs have what can best be described as "super extraterritoriality." They can be enforced extraterritorially, against companies headquartered outside the UK, requiring them to engage in conduct at their facilities outside the UK, that comprises the security of their users outside the UK, even if those users are not UK citizens or residents.

Encryption is an essential tool for combatting today's increasingly sophisticated cybersecurity threats, including those from state-sponsored hacking campaigns like the Salt Typhoon attack that targeted critical infrastructure and government agencies. Introducing a back door into end-to-end encryption means introducing systemic security flaws, as the UK knows, and back doors into encryption jeopardize all users' privacy and cybersecurity because criminals specifically look to exploit these vulnerabilities. Across the world, cybersecurity experts agree that there is no way to provide government access to end-to-end encrypted data without breaking end-to-end encryption and introducing vulnerabilities that could be exploited by anyone, not just law enforcement.

In February 2025, the Washington Post reported that the UK Home Office issued such a TCN to Apple, seeking to compel the company to introduce a back door into its end-to-end encrypted cloud storage service, "Advanced Data Protection" (ADP). This back door access would allow UK officials to require Apple to provide in decrypted form content that any user worldwide had uploaded to the cloud using ADP. Apple is the world's second largest provider of mobile devices. Compelling back door access into its encrypted cloud storage service would mean putting millions of users at risk across the globe. The most harmful impact would fall on those who rely on encryption because they have the most need for secure communications. They include journalists, lawyers, domestic violence survivors, LGBTQ+ persons, and others. More than 100 civil society organizations, cybersecurity researchers, and industry leaders signed a joint letter organized by the Global Encryption Coalition condemning the UK Home Office's use of its IPA authorities to undermine end-to-end encryption. The letter emphasized that such actions set a dangerous precedent and lead to a less secure and less free Internet for everyone.

Rather than capitulate to the demand, Apple made the principled decision to cease offering ADP in the UK, and appealed the notice to the UK Investigatory Powers Tribunal (IPT), which has the authority to review complaints related to UK surveillance. Because of amendments adopted last year, the IPA requires Apple to comply with the TCN even while an appeal is pending. As a result of this obligation and the authority the UK claims to enforce its laws on a global basis, British authorities may insist that Apple build a back door to ADP even though it no longer offers ADP in the UK.

Under the IPA, the UK Home Office has likely prohibited Apple from disclosing the existence of its demand, and Apple has not publicly acknowledged its existence despite widespread media reporting. To make matters worse, the appeal process is also shrouded in secrecy. This means the UK Home Office can place Apple, or any other service provider, under a strict gag order when it issues a TCN. The chilling result is that the public does not know which providers of other encrypted services have received such notices, and if so, which of them complied with those notices, putting user data at risk.

Apple won a significant procedural victory in April when the IPT rejected the government's attempt to keep the litigation entirely secret. According to the judgment, the Home Office argued that revealing the existence of the claim, as well as the names of the parties involved, would be damaging to national security. But the IPT disagreed, citing widespread media reporting, written interventions from civil society organizations, and a letter from members of the U.S. Congress. The judgment officially confirmed for the first time that the IPT was hearing a case brought against the Home Office by Apple over the power to issue a TCN under the IPA. However, nothing more than the bare details of the case were confirmed. The case remains ongoing.

The IPT has also confirmed that it will hear challenges from two UK-based civil society organizations, Liberty and Privacy International, related to the Home Office's alleged decision to force Apple to give the UK government access to users' private data stored on the cloud. Liberty and Privacy International are also challenging the authority of the UK government to issue TCNs at all. Though the case is ongoing and could ultimately result in a decision that protects Apple's encrypted cloud back up service, the DOJ and Congress can act to promote or to ensure that result.

What the DOJ Should Do To Protect Americans' Data Security Against Attack By Countries That Benefit From CLOUD Act Agreements

Although the UK's TCN to Apple was issued under its domestic legal authorities, and not the CLOUD Act or the UK-U.S. CLOUD Act Agreement, the Agreement effectively enables the UK to issue such orders to Apple. The Agreement allows the UK to compel U.S. providers like Apple to disclose user content directly, bypassing the traditional and bulky MLAT process and its requirement for U.S. judicial oversight. This deprives U.S.

companies like Apple the opportunity to challenge the order in U.S. courts under substantive U.S. laws that do not authorize orders like the UK's TCNs, and offers a streamlined path for foreign officials to access Americans' private data. Furthermore, the Agreement permits real-time interception, which MLATs do not allow, further incentivizing UK surveillance orders on U.S.providers.

If Apple is forced to build a back door to ADP to facilitate UK surveillance, UK officials would exploit that opportunity without meaningful transparency. The combined effect of a secret TCN, the access to data held by U.S.communications service providers that is enabled by the Agreement, and the asserted global reach of UK surveillance law would create a powerful tool for surveillance worldwide, with virtually no accountability to users, and limited accountability to the U.S. government.

If the UK insists on using secret orders to force U.S. companies to undermine encryption and thereby put at risk the data of Americans and other people around the world, the DOJ can and should terminate the Agreement or require that it be modified to prohibit orders that force providers to build a decryption capability for encrypted services. Under the terms of the Agreement, the U.S. can unilaterally terminate it without cause and with only 30 days notice. Hopefully, the threat of termination would lead the UK to accept the prohibition on decryption orders.

Terminating the Agreement would have far more severe consequences for the UK than the U.S. In November 2024, around the Thanksgiving congressional recess, the U.S. Department of Justice (DOJ) quietly recertified the Agreement, as required by the CLOUD Act.[2] It did so without fully disclosing to Congress information about the UK TCN authority and how it was likely to be exercised. The DOJ's recertification report provided several key insights about the UK's conduct under the Agreement, not least that the UK issued more than 20,000 requests to U.S. service providers over the two years in which the Agreement was in effect. The bulk of those requests included wiretapping surveillance. In comparison, the U.S. issued a mere 63 to British providers, mostly for stored data. Twenty thousand is an astounding number of wiretaps for criminal cases. In contrast, federal and state law enforcement authorities in the U.S. (which has five times the population of the UK) obtained wiretap orders in criminal cases in only 4,507 instances in the two-year period covering calendar years 2022 and 2023, the most recent years for which data is available.[3] On top of this imbalance, the

[2] The DOJ's "recertification" that a CLOUD Act agreement continues to satisfy the CLOUD Act's § 2523(e) requirements does not serve to extend the "termination" date of that agreement. Rather, the termination date is established in each individual CLOUD Act agreement. Recertification every five years after the Attorney General's original certification is required by Congress to compel the DOJ to regularly re-assess foreign countries' compliance with CLOUD Act obligations. The UK-U.S. CLOUD Act Agreement provides that it will terminate five years after October 3, 2022, the date on which it entered into force, unless terminated earlier by one of the parties with 30 days notice.

[3] Administrative Office of the U.S. Courts, Annual Wiretap Reports issued in 2023 and 2024, covering wiretaps reported in the prior year in each case. This figure combines the number of wiretap orders

DOJ admitted in its Thanksgiving-time recertification to Congress that the U.S. is not getting what it bargained for in the Agreement: a substantial reduction in the number of MLAT requests the UK has sent to the U.S. Processing those requests requires a substantial expenditure of DOJ and judicial resources to secure court orders for crimes that usually occur outside the U.S. and involve non-US person perpetrators and victims.

The dramatic imbalance in the value of the Agreement to the U.S. as compared to the UK owes to the concentration of major communications service providers in the U.S. It demonstrates the overwhelming importance of the Agreement to the UK and its relative lack of importance to the U.S. The U.S. draws some benefits from the Agreement that go beyond the numbers. To the extent the UK engages in surveillance, the product of which is used to disrupt global trade in drugs, the proliferation of nuclear weapons and other transnational crimes, the Agreement makes Americans safer. Moreover, the Agreement relieves pressure that the UK would otherwise apply to U.S. tech companies to compel them to make disclosures that are required under UK law or to store data in the UK ("data localization") to bring it within UK jurisdiction. In other countries, those pressure tactics include fining tech companies for non-compliance with surveillance orders, and arresting and imprisoning their officials until disclosures are made. Terminating the Agreement could invite such pressure tactics.

In deciding whether and how to terminate the Agreement or require that it prohibit decryption orders for encrypted services, the DOJ should weigh the effect such a step might have on the conduct of other countries that have or are seeking CLOUD Act agreements. The UK is not alone in having legal authority to compel companies to assist with surveillance. Authorities in Australia, the only other country that currently benefits from a CLOUD Act agreement, are also statutorily authorized to issue similar technical assistance and capability notices under Australia's Telecommunications and Other Legislation Amendment (TOLA) Act. Like the UK's TCN authority, TOLA allows Australian authorities to require providers to make changes to their systems to ensure access to encrypted communications. While both laws authorize secret demands to weaken encryption, there are some differences. Australia's law explicitly prohibits requiring a provider to build in a "systemic weakness" or "systemic vulnerability," though the statute fails to define these terms clearly, and critics argue the exception is too vague to be effective. The UK IPA, by contrast, imposes no such limitation. If the DOJ moves to terminate or modify the Agreement with the UK, it should consult with

issued by federal and state courts in criminal cases. Some wiretaps issued under intelligence surveillance authorities are issued primarily for criminal purposes. But, even when all of the 606 FISA wiretapping orders reported by the DOJ National Security Division for the two most recent years for which data is available are added to the criminal wiretapping orders, the UK's 20,142 orders dwarf 5113 wiretapping orders sought by federal and state authorities in the U.S. The comparison between the two countries' laws is further complicated by the fact that a small portion of the surveillance orders issued under FISA Section 702 may have been issued in circumstances in which a criminal wiretap order could have been obtained, and are not included in this comparison.

Australian authorities about their use of technical assistance and capability notices to assess whether they are being secretly used to compromise encryption.

What Congress Should Do To Protect Americans' Data Security Against Attack By Countries that Benefit from CLOUD Act Agreements

Congress should amend the CLOUD Act to prohibit agreements with countries whose laws authorize them to mandate backdoors to encryption, and it should require that CLOUD Act agreements prohibit the imposition of such backdoors on any U.S. provider.

To effectively safeguard encrypted services, Congress should amend the CLOUD Act to prohibit CLOUD Act agreements with countries whose laws or practices permit orders that compel providers to build back doors to encryption. This would cut the problem off at the source by preventing the U.S. from forming partnerships with governments that undermine encryption. While a country could later change its laws and violate this requirement, the permissive termination provisions that now appear in CLOUD Act agreements, as well as the requirement of periodic DOJ recertification, should deter such conduct.

Requiring foreign governments to change their domestic laws, particularly as applied to non-U.S. providers, is ambitious. But it is entirely consistent with the DOJ's original pitch to Congress when it proposed the bill that became the CLOUD Act. The DOJ claimed that the law would incentivize adoption of pro-privacy and civil liberties reforms in other countries by conditioning access to data held by U.S. providers on meaningful human rights protections. In fact, the UK enacted legislation specifically to enable its compliance with the CLOUD Act. Conditioning agreements on non-interference with encryption would be a natural and principled extension of that logic and would help ensure that the CLOUD Act promotes, rather than undermines, global cybersecurity norms.

At a minimum, Congress should amend the CLOUD Act to require that CLOUD Act agreements include a provision indicating that while the agreement is in force, the foreign government will not issue orders to U.S. service providers that require undermining encryption. This approach would create clear contractual guardrails, enforceable through the agreement's termination provisions. Its effectiveness would depend on political will and enforcement by the DOJ. As it stands, the UK-U.S. CLOUD Act Agreement contains no provisions addressing encryption, which is a dangerous oversight. Requiring future agreements to explicitly prohibit foreign governments from compelling communications service providers to undermine the security of the communications they carry would be a meaningful reform.

Congress Should Consider Other Amendments to the CLOUD Act

Beyond addressing back doors to encryption, Congress should consider adopting additional amendments to the CLOUD Act to better protect privacy, due process, and human rights. First, the law should be revised to require that all foreign surveillance orders issued pursuant to a CLOUD Act agreement be *authorized* by a court or by another independent tribunal. Instead, the CLOUD Act currently provides that such orders be subject to subsequent independent review or oversight after the surveillance has occurred and when damage to privacy is already done. Judicial authorization requirements are not unique to the U.S.: the Grand Chamber of the European Court for Human Rights in *Zakharov v. Russia* indicated that "the authority competent to authorise the surveillance" must be "sufficiently independent from the executive" (para. 258) to survive review under Article 8 of the European Convention on Human Rights, which protects the right to privacy.

Congress should also require a stronger factual basis for surveillance orders issued under CLOUD Act agreements. They need not meet the strong evidentiary standard that pertains in the U.S. — the probable cause requirement — which is unique. But the current evidentiary standard in the CLOUD Act is excessively weak and malleable: it provides that orders must be "... based on requirements for a reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation." 18 U.S.C. 2523(b)(4)(D).

To strengthen oversight and accountability, Congress should also require transparency and notice. U.S. providers who challenge orders should not be constrained by gag orders that bar them from revealing that they have received such orders, including revealing such a fact to the U.S. government. People who have been subject to surveillance under an order issued pursuant to a CLOUD Act should receive notice of such orders, which notice can be delayed if contemporaneous notice would thwart an investigation.

One might think that if these requirements were added to the CLOUD Act, that they would not protect Americans because the CLOUD Act prohibits the targeting of Americans by orders issued under a CLOUD Act agreement. But, as the members of this Subcommittee know from their work on Section 702 of the Foreign Intelligence Surveillance Act, surveillance that targets people abroad can incidentally or mistakenly pick up communications of Americans who are communicating with the foreign targets. Congress will never know how many Americans' communications were picked up in the 20,000 wiretaps the UK placed under the auspices of its CLOUD Act Agreement with the U.S., but it can be confident that stronger standards and the obligation to give notice would reduce that number.

The U.S. Should Get Its Own House in Order to Protect Encryption

While the UK's demand that Apple undermine end-to-end encryption is deeply concerning, it is not entirely without precedent, even in the United States. Although CDT believes that current U.S. law does not permit the government to issue an order like the one Apple received under the UK's IPA, past action by the U.S. DOJ suggests that the DOJ may have a different view.

In 2015, during the Obama administration, the DOJ sought an order under the All Writs Act to compel Apple to create a modified version of its iOS operating system that would enable the FBI to bypass built-in security protections on an iPhone used by a suspect in a shooting in San Bernardino, California. The case became a flashpoint in the national encryption debate, with Apple refusing to comply on the grounds that the order would set a dangerous precedent and weaken security for all users. Although the FBI ultimately withdrew the request after gaining access to the device through other means, the legal question was never resolved.

Whether the DOJ today, or in a future administration, would take the same position is unknown. For that reason, Congress should amend U.S. law to make clear that the All Writs Act does not authorize the government to compel a provider of a communications service or the manufacturer of a communications device to build in security vulnerabilities, or bypass privacy protections. Providers should be expected to comply with lawful data access requests only to the extent they can do so without compromising the integrity of their systems or devices, or the trust of their users.

Additionally, Congress should clarify that neither the Stored Communications Act nor the Wiretap Act can be interpreted to authorize such mandates. Both statutes include provisions that have been interpreted to require companies to help law enforcement execute surveillance orders.[4] But these provisions are vague and were written decades ago, long before the advent of end-to-end encryption, and should be updated to reflect today's cybersecurity realities. They must not be used as a back door route to impose the same kinds of obligations that Apple is currently fighting in the UK

Conclusion

The threats posed by the UK's order to Apple, and by similar powers under laws in other countries, illustrate the need to strengthen legal protections for encryption. The CLOUD

[4] *See* 18 U.S.C. § 2518(4) ("An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, [... to] furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception.... *See also* 18 U.S.C. §§ 2703, 2706 (although the Stored Communications Act does not contain an explicit technical assistance provision, its disclosure requirements and reimbursement provisions have been interpreted to require certain forms of technical assistance to help execute orders).

Act currently lacks meaningful safeguards against foreign mandates that compel U.S. companies to undermine the security of their services. Without reform, cross-border data access agreements risk becoming conduits for global surveillance demands that compromise cybersecurity and civil liberties of Americans and other users worldwide.

To address this, Congress should amend the CLOUD Act to prohibit agreements with countries whose laws or practices authorize their authorities to compel providers of communications service to weaken security measures, including encryption. At a minimum, it should ensure that CLOUD Act agreements explicitly forbid such demands. Finally, Congress should also clarify domestic law to prevent similar demands under statutes like the All Writs Act, the Stored Communications Act, or the Wiretap Act.

We appreciate the Subcommittee's attention to these critical issues and welcome the opportunity to work with you to enact legislation that protects encryption, preserves trust in U.S. technology, and upholds human rights and cybersecurity worldwide.

Mr. TIFFANY. Thank you, Mr. Nojeim. We are now going to proceed under the five-minute rule with questions.

First, I would like to recognize the gentleman from Texas, Mr. Nehls.

Mr. NEHLS. Thank you, Mr. Chair. Thank you to all the witnesses that are here today. I want to start posing a question to all of you. In your opinion, does the CLOUD Act and the Executive agreements we have under it with the U.K. and Australia sufficiently protect American communications from foreign surveillance? Please explain why or why not.

I'll start with you, Mr. Salgado.

Mr. SALGADO. No, they do not, and for several reasons. The primary one that the U.K. matter exposes is that they don't do anything to dissuade a foreign government from imposing technical capabilities like we've seen in the U.K., but a whole host of other potential efforts undermine security—back doors, contaminated apps.

There is a whole host of things that a creative investigator could come up with, all that undermine the security of American services. Now, it would also compromise Americans' data. The CLOUD Act is a framework that we could use to protect that.

Mr. NOJEIM. I agree with that. We are focused today on the security risks that the CLOUD Act actually incents countries that have product agreements to demand of U.S. providers. There's a lot of improvements that could be made to protect Americans.

One improvement would be to make it so that the U.S. providers could at least tell their government when they receive an order, like the one served on Apple, that this has happened. Apple is gagged not only from telling the world it received an order, but it can't even tell its home country.

Mr. NEHLS. You mentioned there were 20,000 requests.

Mr. NOJEIM. The 20,000 of these—

Mr. NEHLS. We were at 63.

Mr. NOJEIM. Yes. It's imbalanced, it's imbalanced.

Mr. NEHLS. Yes. Thank you. Ms. Wilson Palow?

Ms. WILSON PALOW. I would agree with my fellow witnesses. I would just add and reemphasize that the CLOUD Act is designed when engaging in Executive agreements with these other countries to make sure that these countries have a surveillance regime that respects privacy and other rights, and clearly the U.K. is not following that here with the TCN, the Technical Capability Notice.

It is obviously a huge invasion into privacy. It is breaking all our security by targeting end-to-end encryption. It undermines our potential free speech rights because of the way that end-to-end encryption can be used by so many to communicate, by opposition groups around the world, by human rights defenders in really tough circumstances. I would say that the U.K. is not really in the spirit of the act at the moment.

Mr. NEHLS. Professor?

Ms. LANDAU. This is mostly a law and policy question, but I will pose a technical version of it, which is that in the 1990s the U.S. Government proposed an encryption scheme for digital communications—digital voice communications—in which the keys would be stored with two agencies of the Federal Government.

This did not go over well. It didn't go over well with industry, it didn't go over well with foreign countries, and it didn't go over well with buyers. When AT&T implemented it, the product did not get bought.

Now, imagine that the U.K. requires that encryption use keys that are stored with the U.K. Government. As far as I can tell—and the lawyers to my right can correct me if I'm wrong—but I don't see anything in the CLOUD Act that would prohibit such a thing. Yet, of course, no American company, no American who has any private business would want to use encryption where the keys are stored with the U.K. Government.

Mr. NEHLS. Mr. Salgado, does the CLOUD Act, do our agreements under it pose an undue or unfair burden on U.S. companies? Why or why not?

Mr. SALGADO. I don't think they impose an undue burden, other than that the companies, as Mr. Nojeim pointed out, are barred from disclosing these things that are coming to them.

The CLOUD Act isn't there to protect them from that. It is a good vehicle for that so that they can tell the U.S. Government. Really Congress ought to have much more information than is provided through the current reporting mechanism.

Mr. NEHLS. Yes. Could the U.K., this Technical Capability Notice to Apple, aggravate that burden?

Mr. SALGADO. It could and I think it has. I think you see the situation with Apple where they seem unable to comment on this.

Mr. NEHLS. What happens if other countries now, they all follow suit with this?

Mr. SALGADO. Yes, that's the problem. It just continues with more and more. Especially if it goes unaddressed by the U.S., that just creates an invitation to continue doing things.

Mr. NEHLS. I have about 25 seconds left.

Do you have any recommendations for future Executive agreements or amendments to the CLOUD Act to lessen that burden on U.S. companies.

Mr. SALGADO. I do. There are several of them laid out in my witness testimony.

First and very simply, we should have a declaration in the agreement that network security and cybersecurity is an essential interest, which is a diplomatic term of art, just like free speech and some others, that carries weight with it.

We can also put some in the conditions to get an agreement, some restrictions on the type of technical surveillance capabilities that partner countries would be allowed to provide, among other changes.

Mr. NEHLS. Thank you all for being here. I yield back.

Mr. TIFFANY. The gentleman yields. I now turn to the Ranking Member, Mr. Raskin, for his five minutes of questioning.

Mr. RASKIN. Thank you, Mr. Chair.

Mr. Nojeim, what is the argument on the other side? What is the U.K.'s interest in doing this? Is there some other way to vindicate their interest, other than the construction of the back door?

Mr. NOJEIM. Their argument would be—first, I think they should be at this table and answering your questions.

That the argument would be that they need access to communications content to fight crimes and prevent crimes. That they would say, "Well, our interest in getting access trumps the privacy interests of everybody in the world." That is what they would have to say.

Mr. RASKIN. Yes. To transpose it to the domestic context, it would mean that the government would have access to all our private conversations, not just technologically, but in person, at a restaurant, walking in the park, right? Because there might be some information they want to get.

Mr. NOJEIM. You might have heard some in law enforcement argue that they are going dark because of encryption.

This is the golden age of surveillance. There has never been more human thoughts available to law enforcement agencies around the world in the history of mankind than today. They get it from social media, they get it from data brokers, they get it from all kinds of sources.

Mr. RASKIN. Thank you. Professor Landau, could you take us through the Salt Typhoon hack on the telecom providers and show us why that episode underscores the importance of creating strong security?

Ms. LANDAU. Sure. None of the technical details have been released by the U.S. Government, so this is a certain amount of speculation. We do know that the telecommunications network, the phone network, has some insecurities.

One of the important aspects of the phone network is that the way that the phone systems interoperate used a model of trust where each of the phone companies knew each other and there were few phone companies and that worked fine.

We don't have a few ISPs, we have thousands of ISPs, we have tens of thousands of ISPs. Way back when ISPs started carrying phone calls—for example, E911, Voice over IP, and there was a requirement, an appropriate requirement by the government to have the ISPs interop, interconnect with the phone system so that when somebody dials a 911 emergency call the phone system can then locate where that person is.

The problem is that ISPs—as we all know, the internet has a great number of insecurities. The hackers use the insecurities that are caused by that interconnection. At the technical level I don't know all the different pieces.

When you send a message, when you text, if you're texting over the phone line as opposed to texting via iMessage or an app that encrypts, if you're texting over the phone line then your message is not encrypted. Once the hackers were into the phone system they could read texts.

The CALEA more greatly centralized wiretaps. It used to be wiretaps were done at the phone's central office, the office five miles down from my house or three miles down from my house. They are now more centralized.

A city will have only a few CALEA sites. If you only have a few sites and you're in the phone system and the hackers are in the phone system, they can more easily access it.

There are all sorts of pieces that were not thought through carefully.

Mr. RASKIN. Thank you very much.

Ms. Wilson Palow, so the so-called Technical Capability Notice, which is the euphemism, I suppose, for creating this gapping back-door entryway into communications, contained a provision that the order itself was secret.

I wonder—first, what purpose did that secrecy condition serve for the government? What does that do to civil liberties and people's reasonable expectations of privacy?

Ms. WILSON PALOW. First, the purpose. Again, I'm speculating because the U.K. Government also has maintained total secrecy around why this order exists.

Mr. RASKIN. They have got secrecy around secrecy.

Ms. WILSON PALOW. Yes, secrecy around secrecy, exactly.

The U.K.'s general idea is that—and this is actually not just in the case of TCNs but certain other, broader powers like interception—is that it really heavily tries to protect the technical capabilities that it has.

By making this order entirely secret, it means that users, others, can't know whether or not there is a back door in a service that is being targeted. The U.K. would say that's necessary for national security.

It completely undermines the ability of everyone else, including Congress, including oversight bodies around the world, including users and concerned civil rights advocates—civil liberties advocates—from being able to question whether or not this is an acceptable violation of our privacy and security.

Mr. BIGGS. [Presiding.] The gentleman's time has expired. Thank you.

I apologize. I was having a vote in another Committee that is, like, a mile away, I had to go do that vote. I apologize for missing some of your testimony. I apologize.

I now recognize the gentleman from Wisconsin, Mr. Tiffany, for his five minutes.

Mr. TIFFANY. Mr. Chair, I was happy to pinch hit.

Ms. Wilson Palow, one requirement of the CLOUD Act to enter into these agreements is it has to be part of the convention on cybercrime. Is that correct? That's my understanding.

Ms. WILSON PALOW. Yes, I believe so, although actually some of the other witnesses may be able to answer that better than I could.

Mr. TIFFANY. With that being the case, that convention also includes countries like Turkiye and South Africa. While the concern is being most pointed toward the U.K., and perhaps appropriately so, Turkiye and South Africa aren't exactly exemplars of protecting people's civil rights.

Should we be concerned about this extending beyond the U.K.?

Ms. WILSON PALOW. Certainly. One of the most concerning aspects of this Technical Capability Notice regime is, of course, the U.K. claims to be able to serve the notice actually entirely outside of the CLOUD Act provision.

Even if a country like Turkiye or South Africa did or did not negotiate an agreement, an Executive agreement under the CLOUD Act, if they had a similar regime in place, as long as that's not blocked by the CLOUD Act or some other U.S. law provision, they

similarly could serve these types of notices on U.S. companies and may have much less respect for rights, as you suggest.

Mr. TIFFANY. Mr. Nojeim, do you have a comment in regard to what I just asked in the comments here?

Mr. NOJEIM. A lot could be done to ensure that the U.S. doesn't enter into agreements with countries that don't respect the rule of law.

For example, the CLOUD Act does not have a requirement that the U.S.—that the country's laws require that there be even judicial authorization of surveillance. That seems like a very basic requirement and yet it's not in the CLOUD Act.

Mr. TIFFANY. It strikes me as I sit here and as we once again see that we have spies among us from China and the surveillance that's gone on, a spy balloon that flew over our country a few years ago, are we whistling past the graveyard of China freedoms that—aren't they the greatest threat here?

Mr. NOJEIM. China poses a huge cybersecurity threat to the United States. If countries like the U.K. can force our providers to disarm by removing encryption protection, then we are more vulnerable to that kind of surveillance and that kind of attack.

Mr. TIFFANY. You're saying that we would benefit by amending the CLOUD Act to make sure that it's not abused by the U.K., but perhaps other countries also. Is that what you're saying?

Mr. NOJEIM. Yes. Think of the CLOUD Act requirements in three buckets.

There are the criteria that the country's laws and practices must meet. You could include a new one for protecting encryption.

There are criteria that the agreement must include things that the agreement must say. Right now, the statute says that the agreement has to be silent on encryption basically. It should say it has to protect encryption.

Then, there's requirements about what the orders can and can't do. Amendments in those three buckets could protect encryption.

Mr. TIFFANY. Mr. Salgado, were you with Google in 2018 when the CLOUD Act was enacted into law?

Mr. SALGADO. I was, yes.

Mr. TIFFANY. In reading your testimony, I get the impression that you were a strong advocate for the CLOUD Act at that point. Is that right?

Mr. SALGADO. That's true.

Mr. TIFFANY. Now coming to us saying it needs to be changed.

Did you sense in 2018 that there should be—that we should be really concerned about—that we were giving away too much with that CLOUD Act in 2018? Did you have any concerns at that time?

Mr. SALGADO. I did. There were some changes to the CLOUD Act I would have liked to have seen or some provisions I would have liked to have seen added. There wasn't anything quite on the horizon that we have with the U.K. now.

Yes, there were some things that I thought we could do better with the CLOUD Act. It was pretty good as it was passed and it's been valuable, but it could use a tune-up.

Mr. TIFFANY. This is going to be a pointed question.

It seems to me we have Google and Apple that are the subjects of this, in particular Apple, and we look at them in China and how

they go about doing their business where they have basically, in my terms, they have capitulated to the Communist Chinese Government.

How do you reconcile that as someone who is a former executive with Google?

Mr. SALGADO. I'm not sure I totally understand the question. It may be better directed to somebody who is currently at Google who could explain that further.

Mr. BIGGS. I'm sorry, but the gentleman's time has expired.

Mr. TIFFANY. I yield.

Mr. BIGGS. Thank you. The Chair now recognizes the gentleman from North Carolina, Mr. Knott.

Mr. KNOTT. Thank you, Mr. Chair. I appreciate the topic of today's important hearing.

To the witnesses, I enjoyed speaking with you briefly before the hearing. Again, thank you for making the trip to Washington to discuss this important issue.

It's one that's largely unknown on a technical and a practical level to many in this country, even in Congress. This issue is one that I assume will be abused by foreign governments and/or criminal actors, and hopefully there is a distinction still between those.

Take the U.K., for instance, a country with a proud history of protecting liberties, of respecting the rule of law, adhering to due process, bedrocks of Western civilization.

That country today has protected and built a surveillance State. They spy on their own citizens. They arrest people for posting various things online. They monitor their own citizens' public communications and public posts. It's something that's quite concerning.

Under this particular issue that we're discussing today, I do want to know, just technically speaking, Ms. Landau, can you just explain to us how the communications that are covered that we're discussing today, how they are collected, how are they are stored, and then how they can be accessed in the future?

Ms. LANDAU. The current Google architecture says that if I have three devices that I've made fit this advanced data protection, that when I upload something to the iCloud, it's essentially a message that I am going to send to myself because I might pick it up on another one of my devices.

I have encrypted it end to end, all my devices know the encryption key, and I authenticate to the devices before I pull it down from the iCloud. It's just hanging out in the iCloud, hanging out, hanging out.

Apple doesn't have the key, nobody has the key, just I have the key. That's the protection for it.

Mr. KNOTT. Is the U.K. seeking to collect the data of two parties who are exclusively in the U.K. or is it looking to protect—OK, explain.

Ms. LANDAU. Well, you're probably better set.

Mr. KNOTT. Ms. Wilson Palow?

Ms. WILSON PALOW. Yes. With this Technical Capability Notice they are seeking to open up a back door, so an option to collect data. Then under other surveillance powers that they have, they can collect data from anyone in the world. They have both outward-facing powers and inward-facing to the U.K.

Mr. KNOTT. Then hypothetically, let's say in the future or present, could Federal law enforcement request information from a foreign country like the U.K. to receive communication files that involve American correspondence?

Ms. WILSON PALOW. Yes, I believe that is possible, although I may defer that to some of my other panelists who better understand the American regulations, because I think there are some prohibitions.

Mr. KNOTT. I'm not talking about regulations. I'm talking about—

Mr. NOJEIM. Practically? Yes.

Mr. KNOTT. Practically speaking, that action would be feasible, correct?

Ms. WILSON PALOW. That's right. Because the U.K. absolutely will have Americans' data in the intelligence that it collects.

Mr. KNOTT. It could also be reasonable to assume this is a bypass of Fourth Amendment protections potentially if it was motivated by the wrong actors, correct?

Ms. WILSON PALOW. Again, it potentially could be. In theory there is the possibility.

Mr. NOJEIM. If I could add something here. May I?

Mr. KNOTT. I was getting ready to go to you. Yes, sir.

Mr. NOJEIM. The statute wouldn't permit the U.S. to task the U.K. to listen in on an American. That order would be illegal under the statute.

Mr. KNOTT. Sure.

Mr. NOJEIM. What happens is Americans communicate with people outside the United States all the time.

Mr. KNOTT. It doesn't permit it, but it enables it.

Mr. NOJEIM. It enables it through this kind of incidental collection. You're familiar with this through the 702 program.

If I'm talking to a foreigner abroad who's the target of the U.K. surveillance order, served on Apple, my communications will be collected as well, and then there's rules about when those communications can be shared back to the United States.

Mr. KNOTT. Right. Let me followup with that.

You mentioned earlier this is the golden age of surveillance. What are ways that you believe the CLOUD Act could be reformed to ensure that imminent threats are able to be identified and stopped without eroding the civil liberties protections that we're discussing?

Mr. NOJEIM. In addition to requiring that foreign country have judicial authorization, there ought to be a rule that people get notice when they've been surveilled. We have that rule in the United States. You don't get notice that happens before the investigation has finished, you get notice when it's done.

Mr. KNOTT. Yes.

Mr. NOJEIM. That would go a long way. Also, transparency and the ability of providers to tell their own government that they've received an unlawful order.

Mr. KNOTT. My time has expired, Mr. Chair. I yield back.

Mr. BIGGS. The gentleman yields back. For entry into the record a letter from Reform Government Surveillance.

Without objection, so ordered. I now yield to the Chair of the entire Committee.

Chair JORDAN. Thank you, Mr. Chair.

Mr. Nojeim, should the U.S. Government have to get a warrant before they search the 702 database on an American?

Mr. NOJEIM. Absolutely.

Chair JORDAN. Yes. You were just there. This, the issue we're talking about today, I think even underscores and highlights that reason, because as you point out, the U.S. Government, we spy on foreigners all the time. OK, fine, good. I think that's appropriate.

They pick up all kinds of information on Americans. Then that giant haystack of information gets searched using an American's phone number, email address, or name.

If you're going to do that, go to a separate and equal branch of government, get a warrant, and show that you have a reason to do so.

Mr. NOJEIM. Yes. That's an essential reform and that Congress shouldn't reauthorize Section 702 unless it achieves that reform.

Chair JORDAN. Well, we almost achieved it last year. Last Congress we lost the vote 212 to 212. I'm hoping we win it this time. Mr. Salgado, do you think that's a good change that we need to make?

Mr. SALGADO. It's not only good, it's constitutionally mandated. It's also good public policy.

Chair JORDAN. No kidding. How about Ms. Wilson Palow, do you think so?

Ms. WILSON PALOW. Yes, I would agree.

Chair JORDAN. Professor, do you agree?

Ms. LANDAU. Absolutely.

Chair JORDAN. Wow. This is amazing. This is amazing. We all think we should follow the Constitution and require a warrant if you're going to go search Americans' data.

I am hopeful. This is one of the things that we can get bipartisan support on in this Committee and actually get it. We had it last Congress. Unfortunately, we didn't have quite the votes we needed.

This issue just highlights it even more why that is necessary. Again, I want to thank you all for coming today.

I would yield. I appreciate the gentleman from New York allowing me to go and the Chair for doing so. I yield back the balance of my time to the Chair.

Mr. BIGGS. The gentleman yields.

I now recognize the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you very much, Mr. Chair.

You raised a very interesting point, Chair Jordan: Wanting to make sure that a warrant is obtained to search Americans' data.

I recognize we're focused on the CLOUD Act, and it's an important issue. I don't dispute that. In the times we're in this seems quaint and intellectual, academic discussion. In reality, what we're dealing with is an administration—current administration—that is trying to categorize, gather, and streamline data of Americans with access by a private company.

Now, let me explain a little bit, and I want to ask some questions.

Many of you, I am sure, have heard of Palantir, which is a large data company, has a lot of connections to Elon Musk, to DOGE. In March, Donald Trump issued an Executive Order that would increase the sharing of all unclassified data between and among Federal agencies. It directed agency heads to authorize and facilitate both the intra- and interagency sharing and consolidation of unclassified agency records.

Now, *The New York Times* report in May outlined in great detail how the President has employed Palantir to carry out this Executive Order, essentially to merge all data from all different Executive Branch agencies into one single database.

Now, it's unclear who would control that database, who would have access to it, what searches would be done, and there seem to be no guardrails about that.

Another *The New York Times* article says that the administration—that this database would have 314 different points of data about every American. Literally every American 314 various categories of data will be consolidated into one database by a private company, Palantir.

Now, my colleagues on the other side of the aisle often express concern about government surveillance, about ensuring that we get search warrants in the context of 702, which is a small universe of already obtained information that we know are communications with people of interest from foreign nationalities.

Here, we just have every American's data put into one database with no guidelines and no restrictions. We don't know what Palantir is doing. We don't know what DOGE is doing. We don't know what Elon Musk is doing. It essentially creates a one-stop shop for all Americans' data, which, as we're talking about cybersecurity, I'm sure you all agree that creates a tremendous cybersecurity risk if China or Russia were to hack this.

Now, the Chair of this Committee has said in the past, quote, "Congress has struggled"—of this Subcommittee, Mr. Biggs—"Congress has struggled for four years with a corrupt Presidential Administration"—meaning the Biden Administration—"that further expanded the opportunities for the government to spy on its citizens."

There was nothing in the Biden Administration that approximates this collection of data, this opportunity for the government to spy on its citizens.

I'm not even talking about breaking laws under the Tax Code and sharing tax information with immigration enforcement agencies. I'm not even talking about sharing tax information or Social Security Administration information. This is just every piece of data that is out there in the government's control consolidated with one private company in one database.

I would ask my friend, Chair Biggs, to think about whether, if you are truly worried about government surveillance, why are we not doing any oversight of Palantir, its contracts with the government, its consolidation of all Americans' personal information into one database, and the cybersecurity risks? I really hope, in all seriousness, that you will do oversight over that if you do truly care about government surveillance of citizens.

I yield back.

Mr. BIGGS. The gentleman yields back. Now, I yield myself five minutes.

Mr. GOLDMAN. Mr. Chair, could I—sorry—introduce two unanimous consent requests?

Mr. BIGGS. Yes.

Mr. GOLDMAN. Thank you. One is an April 9, 2025, *The New York Times* article entitled, "Trump Wants to Merge Government Data. Here Are 314 Things It Might Know About You."

The other one is a May 30, 2025, *The New York Times* article, "Trump Taps Palantir to Compile Data on Americans."

Mr. BIGGS. Without objection. Thank you.

Mr. GOLDMAN. Thank you.

Mr. BIGGS. Again, thanks to the witnesses for being here. I'll yield myself now five minutes.

So, Mr. Salgado, in your written statement you said one should take little solace in the provisions of the CLOUD Act. "First, they will still allow for incidental and inadvertent collection of Americans' data, subject to certain minimization requirements."

Can you expand on that for me, please?

Mr. SALGADO. Sure. We touched on that a little earlier in the hearing, specifically Mr. Nojeim's reference to inadvertent and incidental collection where the U.K. can use the CLOUD Act to obtain data from American companies and, inadvertently or incidentally, that data could include U.S. persons' data or data about people in the United States.

As I mentioned in the written testimony, there are restrictions on the U.K. and its use and dissemination of that information, and it has some minimization requirements, which is a phrase you may be familiar with from Section 702 and FISA generally. That's what I was referring to.

Mr. BIGGS. That's what I thought you were referring to. One of the things that I find interesting about that is, having met with the U.K. Home Office within the last six weeks, I am concerned about their processes on what they actually do and their transparency—or lack of transparency—with this incidentally collected data. That's part of the problem that we have with the 702 application as well.

Ms. Wilson Palow, you indicated that you disagree that the U.K.'s safeguards are as robust as they claim, but that is beside the point because your concern about TCNs is that, once a back door is created, States with far less stellar records on human rights, such as Russia and China, could seek similar access through legal process.

You've talked about that a little bit. I'd like you to expand on that. Then, ask each of the Members of the panel to also expand on that.

Ms. WILSON PALOW. Certainly.

Once this back door is built, once end-to-end encryption is broken, any State using their legal process—no matter whether or not it is retrospections as we would hope it would be—can then ask Apple for access to this data, because once it's broken it's not just broken for the U.K. to access the data or for the U.S. to access the data, any country could request it. A lot of countries have surveil-

lance regimes that would allow them to make these sort of requests.

Mr. BIGGS. It isn't just countries that would request it. It's also rogue actors that might be able to access those back doors as well, right?

Ms. WILSON PALOW. That's exactly right.

Mr. BIGGS. Rather than ask each of you to expand on that, what I'm going to ask instead is, my position would be that DOJ, without immediate transparency and opening up of the process—the TCN that's going on with Apple—that they immediately issue the 30-day termination notice. That's just my position.

Does anybody there agree with me on the panel?

Mr. NOJEIM. That would be a good tactic. They could issue the notice. They say we're going to terminate in 30 days unless you withdraw this order to Apple. I think that makes a lot of sense.

Mr. BIGGS. Yes. It's a leverage point. Yes. Professor?

Ms. LANDAU. I absolutely agree.

Mr. BIGGS. Anybody? Mr. Salgado?

Mr. SALGADO. No, I don't disagree with that at all. There's a lot of negotiating strategies here. This agreement is important to the U.K., and I think they would come to the table.

Mr. BIGGS. Ms. Wilson Palow?

Ms. WILSON PALOW. I agree that this is an important moment to pressure the U.K. because, if we don't push back now, then the U.K. may issue many more of these orders in the future entirely in secret and we won't know about them.

Mr. BIGGS. Yes. That's my point, is that it's hanging out there. We don't know enough about what's happening. The legal term is penumbra—there's a penumbra of information floating around out there that we hear about, but we need to nail it down and really take action on it.

The next step is—and I'm going to ask each of you this. We have a minute left; so, you each have about 15 seconds. What two things do you think we need to do to improve the CLOUD Act?

I'll start with you, Mr. Nojeim.

Mr. NOJEIM. Amend it to make it so that no such order can be issued by another country that gets one of these agreements. Amend it to make it so that a country can't get an agreement unless its laws prohibit such orders.

Mr. BIGGS. Thank you. Mr. Salgado?

Mr. SALGADO. I would adopt Mr. Nojeim's and add two more, one being that the providers be allowed to notify the U.S. Government when they receive orders under this act or Technical Capability Notices; and that Congress receive more frequent reporting from the Department of Justice on the operation of the acts that are in place.

Mr. BIGGS. The oversight. Yes. Ms. Wilson Palow?

Ms. WILSON PALOW. I would adopt Mr. Salgado and Mr. Nojeim's recommendations.

Mr. BIGGS. Thank you. Professor?

Ms. LANDAU. I would adopt all three recommendations.

I would add that, as Mr. Salgado mentioned earlier, cybersecurity and network security be part of the criteria in deciding whether or not to enter into an agreement.

I don't disagree with privacy being fundamental and important, but I think there's a really strong lever about cybersecurity and network security that should be used.

Mr. BIGGS. Thank you so much. We've exhausted our time, which is a crying shame because there's so much more to get at with this subject.

I appreciate each of you and your testimony. It's important testimony.

This is an important—here's the thing about Congress. If there was a bunch of money on the table, this room would be filled and everybody would be here. On this type of issue—which is actually critical to the country and national security—you see what happens. It's a sad, sad revelation about the U.S. Congress today.

We appreciate all of you being here. Thank you so much. We will undertake your recommendations and move forward with those very much. Thank you.

We are adjourned.

[Whereupon, at 11:17 a.m., the Subcommittee was adjourned.]

All materials submitted for the record by Members of the Subcommittee on Crime and Federal Government Surveillance can be found at: *https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=118335*.

○