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.