# In Defense of Tapping the Internet to Keep You Safe

The Cipher Brief
By Levi Maxey
November 29, 2017

**In one month, the authorities provided under Section 702 of the Foreign Intelligence and Surveillance Act (FISA) are due to expire unless reauthorized by Congress. Lawmakers are expected to renew FISA, but may put another expiration deadline on the bill, and also may add limitations on how the government is allowed to use the information it collects,** according to the experts that attended The Cipher Brief's Cyber Advisory Board meeting on Tuesday.

- Section 702 allows the U.S. government, primarily the National Security Agency, to monitor the communications of non-U.S. persons who are reasonably believed to be located outside of the United States, by accessing data provided by U.S.-based technology companies. Proponents said the authorities have proven integral to the intelligence community's core missions of combating international terrorism, transnational crime, foreign espionage, weapons proliferation and cyber insecurity.
- Current and former practitioners contend that even a short lag in the authorities could disrupt ongoing intelligence operations, prompting discussion among policymakers for providing a short fix by extending the provisions as is temporarily, potentially linked to other bills.
- There are currently three separate bills in the works vying to reauthorize different versions of the controversial authorities: the FISA Amendments Act of 2017 has been introduced in the Senate and the most likely candidate; the USA Liberty Act and USA Rights Act have been introduced into the House of Representatives.
- Collection under 702 takes place on internet exchange points and server farms within U.S. borders, due to a variety of technical reasons as a result of how data transits the globe on a borderless internet, and the fact that foreigners, including terrorists, often use U.S.-based communications platforms such as Google, Yahoo, AOL, Hotmail, Microsoft and Apple to communicate from countries such as Afghanistan, Syria, or even Russia.

- This is accomplished through two methods: downstream and upstream collection. Downstream collection is the collection of stored communications data, both metadata and content, using "selectors"– such as email addresses, names and phone numbers – tasked to internet communications platforms who report back related communications data. Upstream collection, however, is the tasked collection of data in transit – often at data centers and from fiber optic cable landing sites – from internet service providers using specific selectors designed to capture communications of interest from a deluge of internet traffic in motion.

**The intelligence collection enabled by the authorities under FISA 702 has been determined to be one of the most productive sources of intelligence ever afforded to the NSA, former officials on the Cyber Advisory Board said.**

**General Michael Hayden**, former Director, NSA and CIA

"702 is still the most successful SIGINT [signals intelligence] in the history of the National Security Agency. We have had no program that has produced as much intelligence as this program. But it is all the peripheral questions now – everyone agrees that the core is real."

- Collection under 702 has been particularly effective in identifying dispersed networks of individuals involved in terrorism as determining those who are in contact with known terrorists can help identify previously unknown affiliates. Examining the communications of terrorist oversees has always been the explicit rationale for Section 702 collection, but it is also useful for counterintelligence, counterproliferation, and cybersecurity missions.
- These authorities also benefit U.S. allies as actionable intelligence gathered under 702 authorities has been shared with them.

**Robert Hannigan**, former Director, GCHQ

"I think people pretend to forget that 702 is incredibly important to U.S. allies. I can't think of a major terrorist investigation over the last few years that has not involved the use of 702 materials. We rely hugely on that. Obviously, renewal is an issue for the U.S. – this is a U.S. authority – but it is worth saying that U.S. allies rely hugely on 702 for our own safety."

**Rick Ledgett**, former Deputy Director, NSA

"The principle purpose and the desired outcome is preventive – identify activity, identify people who are involved in planning some activity that we don't know are involved in a terrorist attack and ideally being able to disrupt it in some way through police action or through another nation's action or through military action. By the same token, it is also protecting our forces and our people overseas. We can use it to determine that someone is planning a suicide bombing attack or an ambush of some kind, and then we obviously get that information out as quickly as possible to try to prevent it. It is also useful in forensics after the fact. But this is not just what happened in this particular event, but who were the people that they were working with, and are there other plots? Is this part of a larger plot? This then gets you back into the preventive. It works both ways."

**Incidental collection of U.S. persons' data, as the term implies, at times occurs under 702 authorities.** There are always two ends of a conversation with one being a foreign intelligence target and the other potentially a U.S. person.

- "After a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, NSA has decided to stop some of its activities conducted under Section 702," the signals intelligence agency announced in April. Specifically, the NSA would "no longer include any upstream internet communications that are solely 'about' a foreign intelligence target," meaning that collection will no longer be made if the communicants merely mention a foreign intelligence surveillance target in the content of their correspondence. The reason? Merely collecting based on a selector in the content of the communications – rather than those sent to or from a foreign intelligence target – vastly increases the chances of collecting data belonging to U.S. persons. Currently, this ending of "about" collection is a policy decision by the NSA, but it could be legislatively codified under a renewed 702 bill.
- When the communications of U.S. persons are incidentally collected, and it is determined to be of foreign intelligence value, they undergo a minimization process whereby the identities of the American communicants are "masked" and displayed as U.S. Person 1, for example. Should analysts or policymakers require the identity of a U.S. person to understand the context of the intelligence, they can request that it be unmasked and narrowly disseminated. Since January, the NSA can now share raw 702-collected intelligence prior to minimization to other U.S. intelligence agencies, including the CIA and FBI.

- Incidental collection is not always undesirable. One former intelligence official and Cyber Advisor noted that it can help the FBI and Department of Homeland Security determine if an American citizen or U.S. company has been the victim of foreign cyber attacks – as they are sometimes swept up in the incidental side of the collection. This could inform private industry should they become the victim of advanced nation-state hackers, such as the 2014 Sony Pictures attacks by North Korea, or the 2012 Iranian attacks against the U.S. financial sector.
- To put the scope of collection under FISA 702 into perspective, the NSA collected from 106,469 foreign intelligence targets under Section 702 in 2016, up from 94,368 in 2015. Determining the volume of incidental collection of U.S. persons data, however, is a much more difficult challenge requiring invasive investigation into who the communicants are – email contents and addresses don't often suggest the nationality of the user. But reporting the number of U.S. persons collected that the NSA or others have already identified is feasible and artificial intelligence could play a role in doing such investigations for transparency's sake.

**General Michael Hayden**, former Director, NSA and CIA

"It is a borderless internet, and whether that Gmail account is American or not would require a greater violation of American privacy than just letting it sit in the database."

**One of the most prominent reforms of the current bills introduced in the House and Senate are to close a "backdoor" search capability whereby the FBI is able to query already lawfully collected communications data under 702 with U.S. person selectors for purposes unrelated to the initial collection without needing a court order.**

**Robert Eatinger, Jr.**, former Senior Deputy General Counsel, CIA

"While positions on FISA Section 702 cover the full range from not renewing it at all to renewing it without change, the position that seems to have the most momentum is to amend Section 702 by requiring intelligence agencies that store unprocessed FISA 702 data obtain third-party approval, such as from the Foreign Intelligence Surveillance Court before searching that unprocessed data for information on U.S. persons. Since the consequences, good and bad, will be felt by the American people, whether and what trade-offs to make between measures intended to protect Americans' security and measures intended to protect American's privacy are most appropriately the responsibility of the American people's representatives in the Congress."

- To provide an example of how often this occurs, selectors of U.S. persons were queried 5,288 times to retrieve unminimized communications content and 30,355 times to retrieve unminimized information such as metadata in 2016.
- However, requiring more oversight layers can prove dangerous when quick intelligence is necessitated, the experts said. Take, for example, the recent terrorist attacks earlier this month where an Uzbek national living the U.S. named Sayfullo Habibullaevic Saipov ran down pedestrians on the streets of New York, leaving a note claiming affiliation with ISIS. Under current practice, the FBI likely immediately queried already collected 702 databases with selectors affiliated to Saipov – a U.S. person – to determine if he had been in contact with known terrorists abroad, which could also help determine whether there were other attackers about to mount similar operations in the United States. If the queries came back negative, it would allow the FBI to focus resources elsewhere. Mandating that the FBI file for a warrant would require a burdensome process during dangerous times were quick investigation is necessitated, the former officials said.
- There are a few different suggestions on how to deal with "ticking time bomb" situations. For example, the USA Liberty Act proposes limiting the ability of the FBI when querying U.S. person selectors from 702 collected data when it is pursing specifically a criminal case – allowing them only to initially access the metadata, and to get a court order based on probable cause should they desire further investigation – but would not place such limits in a national security situation such as terrorism.

**Chris Inglis**, former Deputy Director, NSA

"If push came to shove on the survival of the 702 authorities for purposes of foreign intelligence hung by a thread, I would say that we should consider going through additional procedure to authorize those queries, when those queries on are U.S. persons. However lawful it might be to pursue a criminal investigation using the traditional methods, this material is collected for purposes of foreign intelligence, so we might want to have an additional check to make sure we are comfortable making that query."

**While much of the discussion taking place around 702 reauthorization concerns civil liberties and national security, the equities of the private sector largely remain publically silent.**

- U.S.-based companies that provide that data could experience backlash from civil liberty-mind customers that might seek out more privacy-conscious platforms. This could also promote users to increasingly turn to encrypted platforms to communicate.
- Internationally, this has prompted other countries, particularly China and Russia, to argue for data localization laws – a protectionist policy – so that the data of their citizens, including those who would constitute a legitimate U.S. foreign intelligence target, would not lie under the jurisdiction of the U.S. government, i.e. in servers within U.S. borders. This could have adverse implications for U.S.-based multinational tech companies who wish to access international markets.

**Matthew Olsen**, former general counsel, NSA, and former Director, National Counterterrorism Center

"It is the case that Section 702 has been such a valuable and effective authority for foreign intelligence collection because so much of the world's communications infrastructure is in the United States. In fact, that is why it was so imperative to have a law like 702 to have the government work with the private sector here to collect those communications. Over time, that is probably going to change. More of the world's communications won't be centered in the West Coast of the United States. But at least for the foreseeable future, the advantage is to the United States and I think that will make 702 continue to be essential."

*Levi Maxey is a cyber and technology analyst at The Cipher Brief. Follow him on Twitter @lemax13.*