***READING 1:*****U.S. customs agents are searching more cellphones — including those belonging to Americans**


U.S. customs agents searched more than 30,000 electronic devices belonging to foreign visitors and Americans arriving from abroad during the last fiscal year. (ANTHONY WALLACE/AFP/Getty Images)

By [Nick Miroff](https://www.washingtonpost.com/people/nick-miroff/) January 5

U.S. customs agents conducted 60 percent more searches of travelers’ cellphones, laptops and other electronic devices during the government’s 2017 fiscal year, according to statistics released Friday by U.S. Customs and Border Protection (CBP).

The agency said it searched 30,200 devices but the inspections affected only 0.007 percent of the 397 million travelers — including American citizens as well as foreign visitors — who arrived from abroad during the 12-month period that ended Sept 30.

CBP published the figures as it issued new guidelines formalizing the way its officers conduct searches and handle the information they obtain. The agency said the increase was not the result of a policy directive, but rather an indication that electronic devices are increasingly viewed as critical sources of information on potential security threats. “In this digital age, border searches of electronic devices are essential to enforcing the law at the U.S. border and to protecting the American people,” CBP official John Wagner said in a statement.

American citizens and other travelers have expressed astonishment and alarm in recent years at requests to hand over their cellphones from U.S. customs officials at airports and border crossings. But CBP said the practice is justified and its standards have been thoroughly reviewed to ensure they are not an unreasonable violation of privacy rights. The agency said it sometimes needs information it obtains from devices to determine the admissibility of foreign visitors, viewing them as potential sources of intelligence on terrorism, child pornography or other criminal activity.

Under the [new guidelines](https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and), travelers who are selected by its officers for additional screening could be asked to unlock their electronic devices for inspection or provide passcodes. They will be asked to disable the devices’ data transmission, according to a senior CBP official who briefed reporters on the changes Friday. Only information physically stored on the device — such as photographs or phone numbers — would be subject to search, said the official, who the agency would not allow to be quoted by name. CBP agents would not be allowed to seek information stored externally or on a “cloud” linked to the device. White House press secretary Sarah Huckabee Sanders outlined President Trump's priorities on immigration reform. (Reuters)

Such inspections would constitute a “basic search,” the agency said. But in cases where officers determine they have reasonable suspicion of a criminal act or potential threat to national security, they may, with a supervisors’ authorization, conduct an “advanced search” by connecting it to other applications and potentially copying its information. Passwords provided by travelers would be destroyed and not retained by the government, the CBP official said.

Sen. Ron Wyden (D-Ore.), a key ally of privacy rights groups, called the new CBP guidelines “an improvement” but said they’re still too intrusive for U.S. citizens. “Manually examining an individuals’ private photos, messages and browsing history is still extremely invasive, and should require a warrant,” he said in a statement. “I continue to believe Americans are entitled to their full constitutional rights, no matter where they are in the United States.”

Last year U.S. civil rights groups [filed suit](https://www.washingtonpost.com/news/the-switch/wp/2017/09/13/agents-are-increasingly-searching-smartphones-at-the-border-this-lawsuit-wants-to-stop-that/?utm_term=.ed63d1d3b2b0) against the federal government in an attempt to curb device searches.

According to the senior CBP official, about 20 percent of the travelers whose devices are inspected are U.S. citizens. The rest are permanent residents, visitors or other travelers whose admissibility to the United States is subject to CBP discretion.

American citizens [who refuse](https://www.washingtonpost.com/lifestyle/travel/how-can-you-protect-your-right-to-digital-privacy-at-the-border/2017/06/08/95c2cf3e-358f-11e7-b373-418f6849a004_story.html?utm_term=.611cce73af7e) to allow their devices to be inspected cannot be denied entry into the United States, but their devices could be retained for up to five days, the official said. In cases where noncitizens refuse the search, they could be denied entry and sent home. CBP said the decision to review a travelers’ electronic device would not be made at random, and would be requested by officers as part of their broader effort to evaluate whether to allow someone into the U.S. Imagery and information that is noncriminal, including political or sexual content, could also be used by CBP officers to determine whether to admit a foreign visitor, the CBP official said.

<https://www.washingtonpost.com/world/national-security/us-customs-agents-are-searching-more-cellphones--including-those-belonging-to-americans/2018/01/05/0a236202-f247-11e7-b3bf-ab90a706e175_story.html?utm_term=.7bfeb965967e>

**READING 1 QUESTIONS: Answer in complete sentences in your notebook on pg 63**

1. A. How many more searches did US customs agents conduct?

 B. The agency searched how may devices but it only affected what percentage of travelers?

 2. Why are they searching more devices and why do they think it is justified?

 3. Agents can ask travelers to unlock their device. What information can they view and what can they NOT view?

 4. What is their legal argument for being allowed to view information on cell phones?

 5. What amendments might these actions infringe upon and WHY?

 6. A. What will happen to citizens that refuse to allow their devices to be searched? B. What about non-citizens?

 **READING 2 QUESTIONS: Answer in complete sentences in your notebook on pg 63!**

7. What is the Foreign Intelligence Survellance Act (FISA) Section 702?

8. Why does this act worry the President, some representatives, and the public?

9. What is surveillance is allowed under section 702 and what is NOT allowed?

10. What is the FISA court and who is on it?

11. What is ONE reason people are for and ONE reason people are against this act?

12. A. What data is collected? B. What amendments might this violate and WHY?

*READING 2:* **The House voted to allow the NSA to keep spying on Americans** Section 702 lives.

By [Alex Ward](https://www.vox.com/authors/alex-ward)[@AlexWardVox](https://www.twitter.com/AlexWardVox)alex.ward@vox.com  Jan 11, 2018, 5:50pm

*Zach Gibson/Getty Images*

A debate over a controversial law that gives the government broad powers to spy on foreigners purposefully and Americans incidentally briefly rocked both the White House and Capitol Hill on Thursday after a disruptive tweet by President Donald Trump.

A section of the Foreign Intelligence Surveillance Act (FISA), [**Section 702**](https://intelligence.house.gov/fisa-702/), allows US intelligence agencies to collect the email communications of foreigners living abroad in order to obtain information about potential threats against the United States. But sometimes intelligence agencies sweep up emails sent by or to Americans, and that worries citizens and policymakers alike who care about their privacy.

It also evidently worries President Trump.

On Thursday morning, as the House of Representatives was about to begin deliberations on an amendment to the law that would help safeguard Americans’ privacy by requiring government officials to request a warrant before looking at information collected from emails by US intelligence agencies — the president posted a tweet criticizing the law:

Panicked Republicans [**considered**](http://www.cnn.com/2018/01/11/politics/fisa-house-vote-congress/index.html) pulling the bill because they thought the president was against it. But about 90 minutes after his first tweet, Trump posted a follow-up tweet that seemed to walk back his opposition to the law:

[](https://twitter.com/realDonaldTrump)**[Donald J. Trump](https://twitter.com/realDonaldTrump)**

[✔@realDonaldTrump](https://twitter.com/realDonaldTrump)

[Replying to @realDonaldTrump](https://twitter.com/_/status/951431836030459905)

With that being said, I have personally directed the fix to the unmasking process since taking office and today’s vote is about foreign surveillance of foreign bad guys on foreign land. We need it! Get smart!

[9:14 AM - Jan 11, 2018](https://twitter.com/realDonaldTrump/status/951457382651056128)

The amendment ultimately didn’t pass, but the House did[**vote to reauthorize**](https://www.washingtonpost.com/politics/trump-backtracks-after-appearing-to-contradict-his-administrations-support-of-fisa/2018/01/11/5d7f7088-f6d1-11e7-91af-31ac729add94_story.html?utm_term=.ff38cb2719c5) the law for another six years by a 256 to 164 margin.

Thursday’s drama is just the latest moment in the years-long controversy over the US government’s ability to collect, store, and even read the emails involving American citizens and residents because of FISA’s Section 702.

Here’s a brief guide on what Section 702 lets America’s intelligence agencies do — and why it’s long been a sensitive issue for Americans in and out of government.

**Section 702 targets foreigners’ emails — but there’s a catch**

Section 702 doesn’t allow intentional surveillance targeting of Americans; rather, targeting of “accounts whose owners are reasonably believed to be foreigners outside of the United States,” Michael Hayden, a former director of the CIA and NSA, told me.

The law is intended to collect information that could potentially stop terrorist attacks by foreigners against the United States, but sometimes the spying programs scoop up Americans’ emails and information along with it.

“Most of the world’s internet traffic passes through portals inside the United States,” said Todd Rosenblum, a top intelligence official at the Department of Homeland Security from 2009 to 2011. Because of that, it’s difficult not to unintentionally collect information from or about US citizens and residents.

Critics believe that violates Americans’ Fourth Amendment right against unreasonable searches and seizures.

The [**FISA court**](http://www.cnn.com/2014/01/17/politics/surveillance-court/index.html) is supposed to be the legal check on the government’s surveillance powers. Made up of 11 judges, the court is who ultimately decides whether or not intelligence officials can look at email content or other data as part of a national security investigation.

Proponents [**argue**](https://www.stanfordlawreview.org/online/is-the-foreign-intelligence-surveillance-court-really-a-rubber-stamp/) that this court serves as a sufficient check on the government’s powers; critics, on the other hand, [**say**](https://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy) the court provides nothing more than a rubber-stamp for whatever the intelligence agencies ask for.

The debate over the FISA court is just one of the many controversies surrounding Section 702. At the core, the question is whether the government should prioritize the security of the American people, or their privacy.

**The privacy versus security battle continues**

Rep. Zoe Lofgren (D-CA) co-sponsored the failed amendment to add new safeguards to Section 702, along with Rep. Justin Amash (R-MI).

“Because of the architecture of the internet, we are collecting vast amounts of data,” Lofgren told me. “Your phone calls, your emails, your text messages, and video messages. And under Section 702 you can search that for Americans and for crimes that have nothing to do with terrorism.”

Privacy advocates also point to the potential for the law to be abused. “Section 702 could too easily be a tool to target government critics, immigrants, and vulnerable communities,” said Neema Singh Guliani, legislative director at the American Civil Liberties Union.

Such cases have happened. In May 2015, for instance, FBI agents [**arrested**](https://www.aclu.org/blog/privacy-technology/surveillance-technologies/chilling-surveillance-and-wrongful-arrest-chinese) a man named Xiaoxing Xi, a Chinese-American physics professor at Temple University. The government claimed he was a Chinese spy after looking at his communications with the FISA Court’s approval. The government dropped the charges four months later because it appeared he was merely contacting colleagues in China. Xi is now working with the ACLU to sue for damages.

Hayden and many others in the intelligence community have a different view of Section 702. On October 23, Hayden and 15 othernational security professionals — including former CIA Director John Brennan and former Director of National Intelligence James Clapper — **[signed](https://www.lawfareblog.com/former-national-security-officials-urge-section-702-reauthorization-letter-congress)**a letter to congressional leaders urging them to reauthorize the email-collection provision.

“There is no substitute for Section 702,” they wrote. “It is the most effective mechanism to protect the US from the very large number of real threats that use American email and Internet services.”

The debate over Section 702 now moves to the Senate, where it will likely not spark the same level of controversy as it did in the House vote on Thursday. So far, senators from both parties have [**signaled**](https://www.nytimes.com/2018/01/10/us/politics/nsa-surveillance-privacy-section-702-amendment.html) they will reauthorize Section 702 without any additional reforms to ensure greater privacy. But the wider debate about striking the right balance between citizen privacy and security is sure to continue.

<https://www.vox.com/2018/1/11/16878220/house-vote-surveillance-spying-fisa>