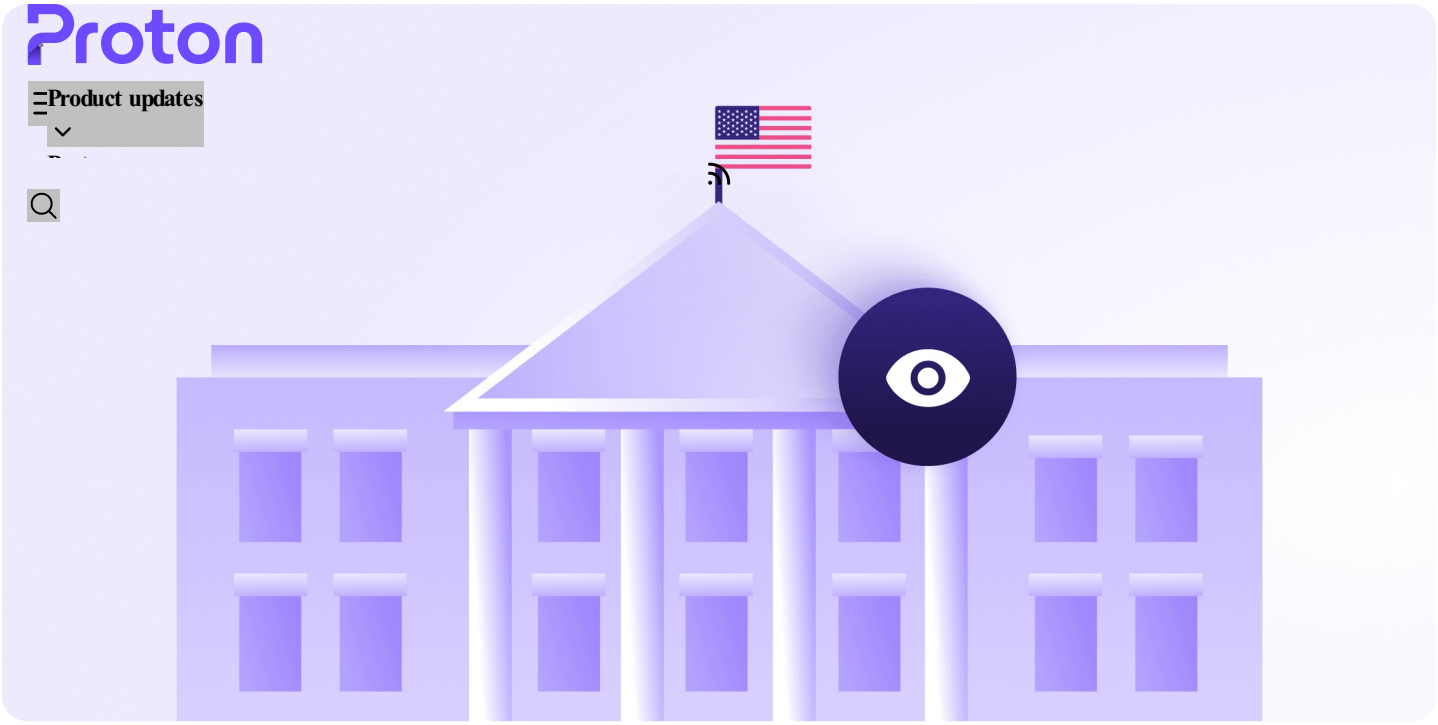


PRIVACY NEWS

Trump now controls the NSA and FBI – What this means for your privacy

Richie Koch

Share

Published on January 27, 2025

The United States claims to be the land of the free, but freedom is impossible without individual privacy. You must be certain the government will not arbitrarily monitor you in your home or on your devices. Yet the US legal system does little to protect your privacy rights. Eight years ago, we wrote about Trump taking control of the NSA, however former President Biden also expanded the surveillance state, signing the law that renewed Section 702 in 2024 (which we also covered).

In general, the US surveillance state has greatly expanded its scope, under both Democratic and Republican administrations. Because of this, we're providing a comprehensive update on how government agencies, law enforcement, and corporations infringe on your data privacy and how you can take actions to protect yourself online.

- What will Trump do about warrantless surveillance?
- How the US warrantless surveillance machine can spy on you
- Big Tech must spy on behalf of the US government
- Warrantless surveillance methods explained

- Section 702
- Geofencing warrants
- Purchase data from data brokers
- National security letters (NSLs)

- How Proton protects your data

What will Trump do about warrantless surveillance?

It's hard to know exactly what President Trump will do when it comes to reforming or deploying warrantless surveillance. Candidate Trump spoke stridently about dismantling the surveillance state, even saying "KILL FISA" just before the US Congress renewed Section 702 with bipartisan support.

However, Tulsi Gabbard, Trump's choice for the Director of National Intelligence, has already walked back her long-standing opposition to Section 702. Furthermore, the intelligence community treats FISA and Section 702 in particular as "crown jewels" and has managed to secure their extension under both Democratic and Republican regimes.

Section 702 comes up for renewal again in 2026, and we'll be watching the developments surrounding it closely.

How the US warrantless surveillance machine can spy on you

Each level of US law enforcement, from federal intelligence agencies down to your local police department, has its own special back door that lets them collect your information without judicial review.

- Most foreign intelligence agencies, like the NSA and CIA, are nominally barred from spying on US citizens or anyone in the USA but still end up collecting their data thanks to Section 702. This data is then compiled into one massive, searchable database.
- The FBI can search Section 702 data, giving it access to data it would normally need a warrant for, and deploy national security letters that force organizations to give up limited info on their clients.
- The FBI, DHS agencies (which include Immigration and Customs Enforcement and Customs and Border Protection), and local law enforcement can all use geofencing, buy data from data brokers, monitor social media, use CCTV footage and facial surveillance technology in public spaces, and more.

Despite all these different programs, nearly all US surveillance has one thing in common: outsourcing. Big Tech is now an integral part of the US surveillance machine.

Big Tech must spy on behalf of the US government

The US government recognized that Big Tech and social media companies rely upon the endless surveillance of everyone, and they're incredibly good at it. Except for TikTok, nearly all Big Tech and social media platforms are American, meaning they're vulnerable to Section 702 requests and national security letters. Every post, photo you've shared or stored, or message you've sent (if you didn't turn on end-to-end encryption) could be used by the government. Essentially, if Big Tech has access to your information, so does the US government.

Warrantless surveillance methods explained

Section 702

Section 702, part of the FISA Amendments Act from 2008, allows the US government to monitor foreign nationals outside the United States without a warrant; however, a "backdoor" permits warrantless surveillance to be extended to people in the US as well. The NSA, for example, can name a foreign national outside the US as the target. If that target speaks with a US citizen or someone in the US, their communications are collected too. The information of thousands of US citizens is collected this way each year. This data is then compiled into one massive database that the FBI can use.

What data is vulnerable?

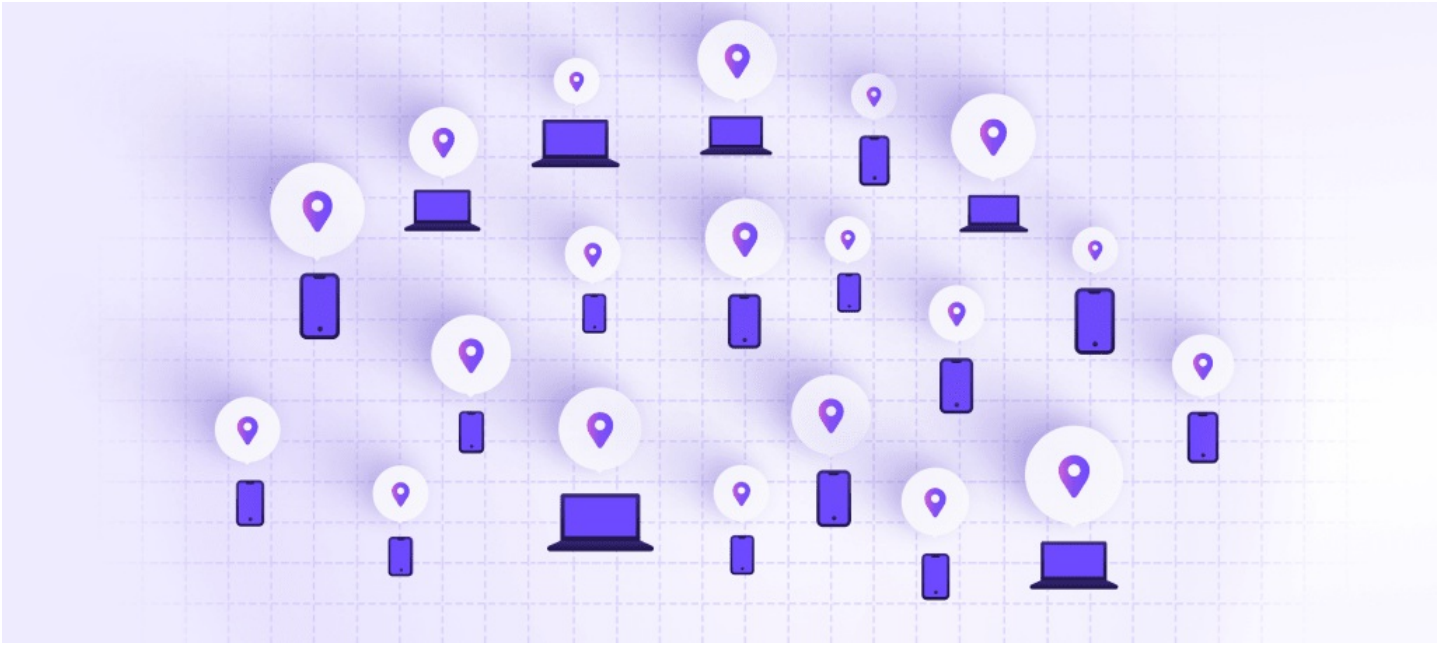
The contents of any communication, be it emails, texts, or phone calls.

How it bypasses judicial review

Section 702 requests aren't reviewed on an individual basis. Instead, each year intelligence agencies (such as the NSA or CIA) submit a "certification" to the Foreign Intelligence Surveillance Court (FISC) that explains the procedures they'll use to collect data. Once the FISC approves an agency's certification, it's pre-authorized to conduct surveillance according to its self-described procedures.

Example

Examples of the FBI inappropriately using the Section 702 database to access Americans' information include searches into participants of **the January 6 Capitol riots** and the **2020 George Floyd protests**. **Big Tech companies** (Google, Meta, Apple, and Microsoft) receive tens, sometimes hundreds of thousands of FISA requests each year. These requests aren't categorized by type, so it's impossible to know how many were done via court orders from the FISC or Section 702.



Geofencing warrants

Geofencing involves creating a virtual boundary around a specific area and obtaining data from all devices within that boundary during a given time frame. Law enforcement agencies have used geofencing warrants to gather location data from smartphones, often implicating people who were in the wrong place at the wrong time.

What data is vulnerable?

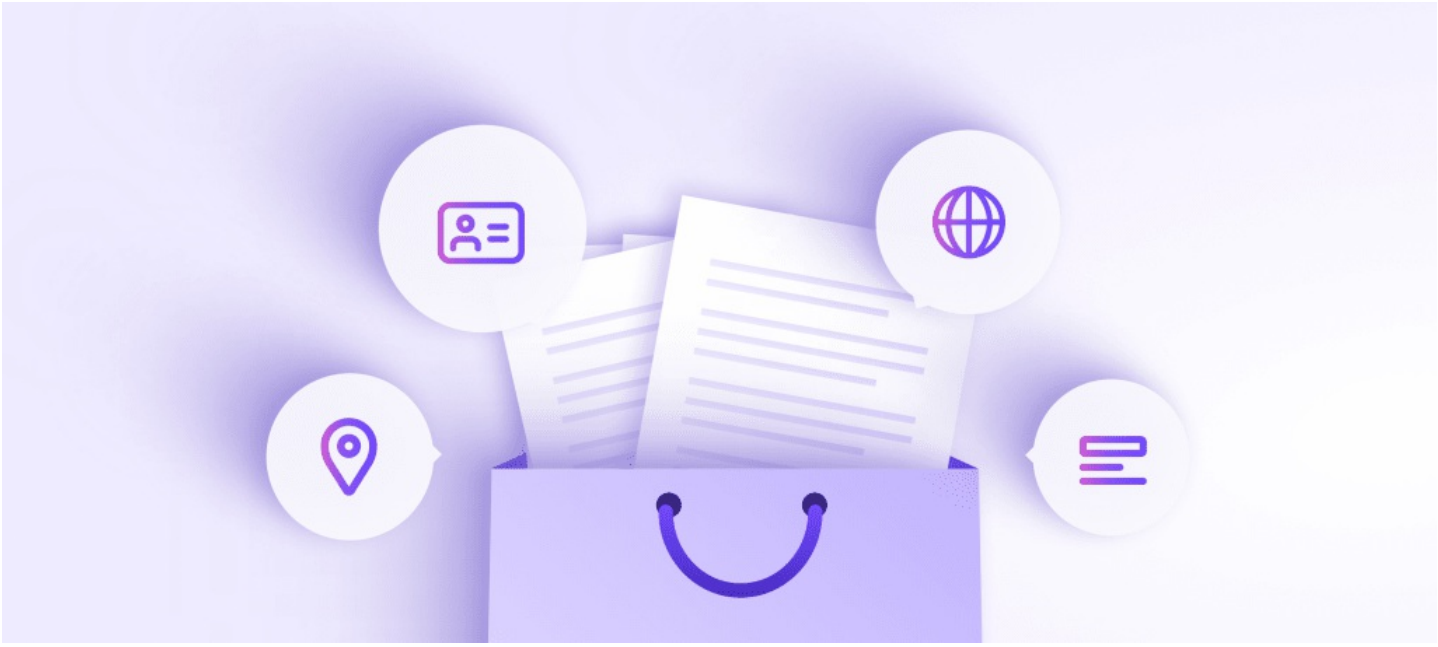
This collects device location data, and you might be surprised at how many apps and services collect this information. Google, which runs Android, is by far the most popular target (it received over 10,000 geofencing warrants in 2020), but Apple, Uber, Snapchat, and other companies also regularly receive these types of warrants.

How it bypasses judicial review

Although geofencing warrants require a court order, the scope of these warrants lack specificity. Instead of targeting a known suspect, they sweep up data from anyone who happened to be in a given area, turning innocent bystanders into potential suspects.

Example

Law enforcement used geofencing warrants to identify participants in **the January 6 Capitol riots** and **Black Lives Matter protests** by obtaining location data from their smartphones.



Purchase data from data brokers

Data brokers collect and aggregate massive amounts of personal data from trackers and services we use every day, like tech

or credit card companies. They then sell this data, which can include location, browsing habits, health information, and more. The government can bypass legal requirements by purchasing this data directly from brokers instead of obtaining it through traditional legal channels.

What data is vulnerable?

Your devices, your apps, and the ad tech underpinning much of the internet collect an incredible amount of personal information, and data brokers compile all of it. Location data, browsing activity, your email address, health information, financial information, your face and fingerprints, and more are all vulnerable.

How it bypasses judicial review

The government doesn't need a warrant or subpoena to purchase data. This practice exploits a legal gray area where third-party data collection is considered separate from direct surveillance, even though the result is identical.

Example

The number and scope of abuses are too broad and too numerous to account for fully. The NSA, Treasury Department, FBI, Department of Homeland Security, and Immigration and Customs Enforcement have all purchased data that they would otherwise need a warrant to collect.

National security letters (NSLs)

NSLs are administrative subpoenas that compel institutions, such as banks, internet service providers, or libraries, to hand over sensitive client data without requiring judicial approval. These letters often come with gag orders, preventing companies from notifying individuals about the data request.

What data is vulnerable?

NSLs allow the FBI to obtain subscriber information for telephones and electronic communications, toll billing information, and electronic communication transaction records. They can also be used to get financial records from financial institutions.

How it bypasses judicial review

NSLs can be issued unilaterally by FBI special agents without any oversight from a judge as long as the information requested is relevant to national security.

Example

Big Tech companies, like Google, Meta, Apple, and Microsoft, have been compelled to hand over user data in response to NSLs. While exact cases are often shrouded in secrecy, these tech giants receive hundreds, sometimes thousands, of NSLs a year.

How Proton protects your data

To secure your right to privacy, you must have both of the following:

- Strong legal protections for personal information and policies that limit the government's and businesses' ability to access it.

- Technological solutions that protect personal information from incidental and illegal seizure.

Proton is protected by strong Swiss privacy laws, such as Article 271 of the Swiss Criminal Code. This forbids all Swiss companies from assisting foreign law enforcement, under threat of criminal penalty. All requests are evaluated under Swiss law by the Swiss government. This is a much higher standard of protection than US-based companies can offer. We also have a long track record of fighting (and winning) court cases to strengthen Swiss privacy laws.

Proton services use end-to-end encryption or zero-access encryption, which makes it impossible for anyone — including Proton — to see the content of your emails, files, photos, passwords, schedules, and more without your permission. This applies to Proton Mail, Proton Drive, Proton Pass, and Proton Calendar. If you use Proton VPN, you can shield your browsing history from ad tech and data brokers. Proton VPN encrypts your internet connection so the websites you visit cannot see your real IP address, and your internet service provider cannot see what websites you visit. Proton VPN's NetShield Ad-blocker lets you block many ad-tech trackers that share your browsing history with data brokers.

Additionally, unlike Big Tech companies, which are only concerned about profits (and it's always most profitable to serve those in power), Proton is primarily owned and controlled by the non-profit Proton Foundation. This legally obligates us to pursue our original mission and ensures we only act in the interest of the Proton community.

Moving to Proton will measurably help protect your information from US government overreach, but only massive legal reform can truly protect the right to privacy in the US.

Richie Koch
Prior to joining Proton, Richie spent several years working on tech solutions in the developing world. He joined the Proton team to advance the rights of online privacy and freedom.

Related articles

JAN 31, 2025PRIVACY NEWS

DeepSeek? More like DeepSneak

Not only does DeepSeek collect extensive personal information, but it cannot legally resist government demands for access to that data.

JAN 30, 2025PRIVACY GUIDES

How a family password manager can save parents time

Tired of resetting passwords for your family? Find out how a family password manager can help you save time on password admin.

JAN 29, 2025PRIVACY GUIDES

What is BCC in email? How to safely use it

What is BCC in email language? Here's what BCC means, how it works, and when and why you might want to use it.

JAN 24, 2025OPINION

Our predictions for the internet in 2025

See our predictions for the internet in 2025, from AI cyberattacks to DIY surveillance.

JAN 24, 2025PRIVACY GUIDES

How to view your saved passwords easily — and privately

Saving passwords in a password manager can help you stay safe online, but how can you see all your saved passwords in one place? Find out with Proton Pass.

JAN 24, 2025PRIVACY GUIDES

Email password 101: Fully secure your inbox with 2 simple solutions

Learn how to secure your email password and inbox with strong passwords, 2FA, passkeys, and tips to prevent data breaches and unauthorized access.

Proton AG

Route de la Galaise 32
1228 Plan-les-Ouates
Geneva, Switzerland

Products
+
Privacy and community
+
Company
+
Connect
+

System status
Report abuse
Report a problem
Report a security issue
Request a feature
Privacy Policy
Terms & conditions
Transparency report