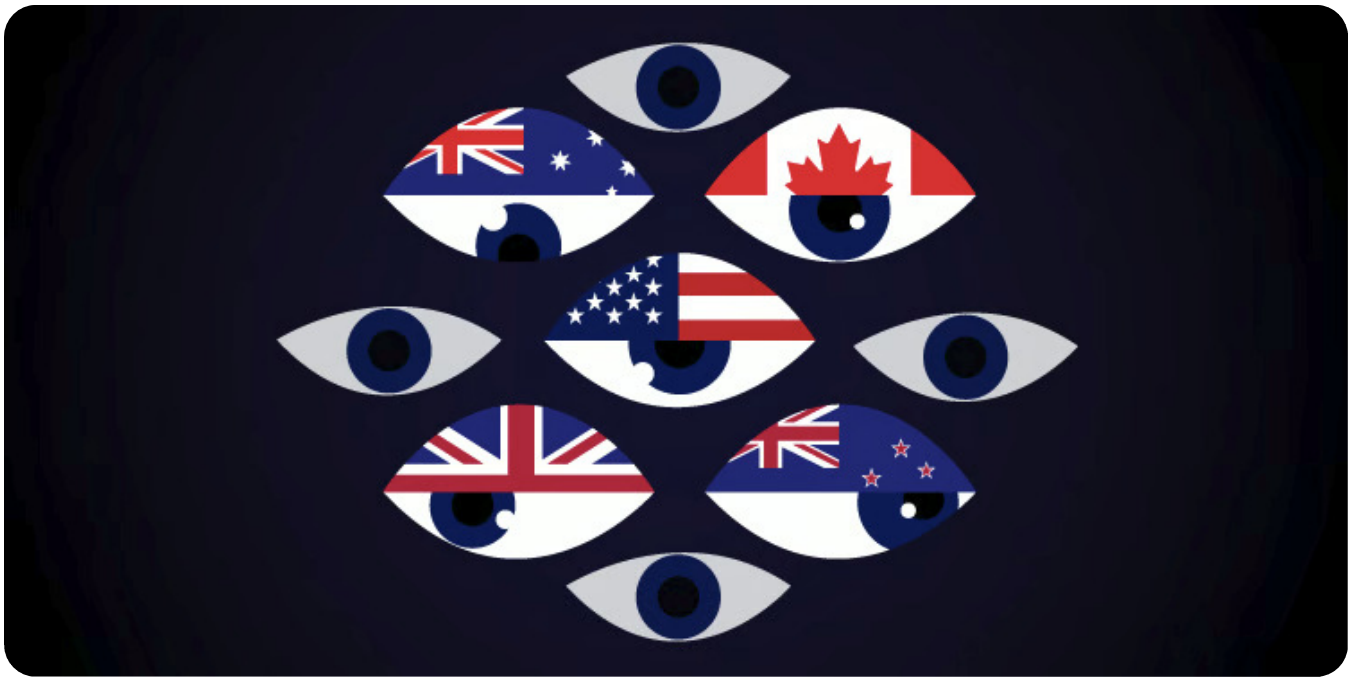
# Five, Nine, and Fourteen Eyes alliances explained



Šarūnas Karbauskas Senior Tech Content Writer

December 18, 2020 • Updated: April 22, 2025 • 7 min read

Audio Coming Soon

Instaread

Nowadays, it's clear that people's privacy isn't a priority for most organizations because there's so much to gain from tracking users online. From large tech

companies wanting to monetize our activities, to government agencies surveilling their citizens for the sake of national security – the rise in widespread surveillance is prevalent everywhere.

In this article, I'll explain the **Five Eyes alliance, its extensions, and how their existence impacts our daily online lives**. Briefly put, it's an alliance between various countries that share intelligence and data collected about their citizens between member states. Knowing about its existence, you should be more careful about what services you choose to enhance your online anonymity.

## 5-Eyes alliance

The Five Eyes alliance (FVEY) consists of the five parties to the UKUSA Agreement:

- **The US**
- **The UK**
- **Canada**
- **Australia**
- **New Zealand**

The goal of this agreement is to provide a framework for sharing signals intelligence data among its signatories. To understand the Five Eyes, it's essential to know what signals intelligence (SIGINT) is. Broadly speaking, this term defines intelligence obtained through the interception of transmission signals and has more specific subsets:

- **Communications intelligence (COMINT)** – interception of various communications between people, like telephone calls and text comms like emails and text messages
- **Electronic intelligence (ELINT)** – use of electronic sensors to signals unrelated to communication, e.g., signals from radars or surface-to-air missile systems
- **Foreign instrumentation intelligence (FISINT)** – a subset of electronic

intelligence that focuses on intercepting and analyzing foreign signals used for operating various devices like satellites and aircraft

Five Eyes countries have intelligence agencies like the **NSA (National Security Agency from the US)** or **GCHQ (Government Communications Headquarters from the UK)** spying on people in various parts of the world and sharing it with each other.

Although these activities are **mainly directed towards geopolitical adversaries** (China, Russia, Iran, etc.), no country is truly exempt from such surveillance. In fact, documents leaked by Edward Snowden reveal that the **US is paying UK's GCHQ to gather data on US citizens** and share it with the NSA – although warrantless "wiretapping" of citizens is illegal, the UKUSA Agreement offers a workaround to do it anyway.

Born out of the Atlantic Charter in 1941 (formalized as the BRUSA Agreement in 1946, which later became known as UKUSA), the Five Eyes had the objective of monitoring the Soviet Union and its allies. However, the alliance's targets and powers changed as the political landscape changed. Crucially, there has been a steady shift towards collecting private communications (particularly during the "War on Terror").

## 9-Eyes alliance

The Nine Eyes is an extension of the Five Eyes and consists of the following countries:

**Five Eyes states** +

- **Denmark**
- **France**
- **The Netherlands**
- **Norway**

Little is known about how the rights and responsibilities of the Nine and Five

Eyes countries differ. However, these additional states are not exempt from surveillance within the alliance.

## 14-Eyes alliance

The Fourteen Eyes are a further extension of the UKUSA Agreement, known as the **SIGINT Seniors Europe (SSEUR)**. The countries belonging to it are:

**Nine Eyes states** +

- **Belgium**
- **Germany**
- **Italy**
- **Spain**
- **Sweden**

This is another group of states adjacent to the Five Eyes inner circle. The specific details of the agreement between them are not fully known.

## What are third-party contributors?

Aside from the Fourteen Eyes country groups, there are other contributors to the UKUSA Agreement alliance. These countries share with and receive intelligence data from the Eyes group, but have fewer rights and responsibilities. These third-party allies usually undertake partial intelligence sharing to combat specific threats.

Third-party allies are believed to include countries belonging to **NATO** (Iceland, Greece, Hungary, Romania, the Baltics, and many other European countries), as well as other strategic allies – **Israel, Singapore, South Korea, Japan**, and more.

## How does the Fourteen Eyes alliance affect your privacy?

The Fourteen Eyes alliance is essentially a global surveillance alliance, which has far-reaching implications for personal privacy. The full extent of how much the intelligence agencies in these countries know about you is vague, but Snowden's leaks and other media stories make it clear that your online activities, phone conversations, and other sensitive information are all fair game.

For example, the global ECHELON program uses communications satellites to intercept your private communications, which are then stored and analyzed. Meanwhile, the **PRISM program collects the private communications data of US citizens from tech companies like Facebook, Google**, and others.

Aside from sharing private communications data cross-border, the Five Eyes countries have been responsible for a wider push to undermine privacy. The most notorious example is the **USA PATRIOT Act of 2001**, which has allowed an unprecedented level of surveillance on US citizens. But the US (sadly) doesn't have a monopoly on mass surveillance:

- **In 2016, the UK passed the Investigatory Powers Act** (affectionately known as the Snoopers' Charter), giving intelligence agencies the mandate to collect bulk communications data of citizens, and requiring ISPs and telecommunications companies to store data on users
- **In 2015, Australia passed a similar law, the Telecommunications (Interception and Access) Amendment (Data Retention) Act**. Among other things, it requires ISPs to store user data for a period of 2 years

UKUSA Agreement countries have also pushed for an end to encryption and have advocated other privacy violations in the service of "security."

## 3 reasons to avoid the Five Eyes

ISPs have been doing the dirty work of intelligence agencies and law enforcement for years. That's why people have turned to VPN services, secure email services, and encrypted messaging apps to reclaim their privacy. Unfortunately, if you're using a service based in a Five Eyes country, there's

only so much privacy you can get from it.

### 1. Five Eyes against end-to-end encryption

In 2018, the Five Eyes nations released a statement saying they would try to **force tech companies to provide encryption backdoors**. Australia has already followed through with a bill allowing government agencies to force companies to hand over user data and create backdoors if that data is encrypted.

While other alliance nations haven't followed in Australia's footsteps yet, they have expressed that intention. For example, US Attorney General William Barr has repeatedly called for a similar bill. And a similar sentiment has been echoed by the UK, Canada, New Zealand, and others.

In 2025, Britain demanded Apple to create a backdoor to user data, which could be a severe security and privacy issue. It's clear that Five Eyes countries are determined to fight against user privacy rights.

As such, VPNs or email services based in a Five Eyes country could be forced to provide access to your data, even if it's encrypted. Needless to say, that may have serious consequences.

### 2. US and UK governments force VPNs to hand over user data

VPN service providers in the US and UK have been **forced to collect and share user data with law enforcement** on a few occasions. An important thing to note is that such an order may be accompanied by a gag order, which means you may be unaware of the danger to your privacy until it's too late.

Here are some examples of that happening:

- **IPVanish**, a prominent US-based VPN, collected and gave user data to an FBI investigation, despite claiming to operate under a no logs policy in 2016
- **Riseup**, a US-based VPN/email provider complied with 2 warrants for user data and were prevented from speaking about it until later due to a gag order

order

- **Lavabit**, a US email provider, closed shop after refusing to give agencies encryption keys in 2013. Ironically, the target of surveillance was Edward Snowden
- **HideMyAss**, a UK VPN provider, collects user data and has given it to the authorities - the company is transparent about this

### 3. User data travels between Five Eyes countries

Imagine you are using a VPN service operated by a UK company. Due to the Snoopers' Charter, the VPN provider would collect data about you and share it with the UK government when necessary. Yet the problem doesn't end there.

Due to the UKUSA Agreement, **your data may end up in the hands of an intelligence agency in the US, Australia, Canada**, or some other party to this treaty.

Those arguing for security over privacy often ask why anyone would care about being watched if they have nothing to hide. The Five Eyes topic is a great illustration because the idea of some foreign intelligence agency knowing your browsing habits feels completely outlandish. Yet the truth is governments are not as benevolent as they seem, and they might get a lot worse in the future. The social credit system in China is a great example of a possible future.

## Most popular cybersecurity services based in Five Eyes nations

The Five Eyes states are some of the most technologically developed in the world. Naturally, they are home to many cybersecurity businesses, including VPN services, password managers, encrypted email services, secure messaging app developers, and more.

Just because these services operate from within the US, UK, or elsewhere in the Five Eyes doesn't necessarily mean they're bad. With that said, if you don't want to take your chances (however slim they may be), keep these in mind.

### Five Eyes VPNs: Private Internet Access, IPVanish, TorGuard,HideMyAss

VPNs are a popular tool in the Five Eyes, especially in the US. It's no surprise that these countries are home to some of the most prominent VPN providers.

3 of these (**PIA**, **IPVanish**, **and** **TorGuard**) are based in the US and of these, PIA certainly has a great reputation among casual users and privacy advocates alike. Why is that?

Well, Private Internet Access has always been adamant about not keeping any user data. Unlike everyone else, however, PIA has been tested in court on several occasions. Proving its no-logs policy in the wild is a powerful statement in the VPN industry – better than any marketing promise.

Unfortunately, some on this list don't have PIA's reputation. IPVanish has been caught logging in the past (albeit this was under a different owner), whereas HideMyAss has to collect user data by law.

***You may also like to read:*** ***Most secure VPN services***

### Five Eyes private email services: Hushmail, Thexyz

Email services may even be more sensitive than VPNs when it comes to privacy. It's fortunate, then, that there are few email services operating from Five Eyes countries. Hushmail and Thexyz are 2 of the most prominent ones – both Canadian.

Of these two Hushmail is the one to look at in more detail. In 2007, the company handed over 12 CDs of emails to the FBI. To quote Wired, the FBI made Hushmail "store the suspects' secret passphrase or decryption key, decrypt their messages and hand [the emails] over." Granted, this isn't specifically related to the UKUSA agreement, but it goes to show the privacy issues in Five Eyes countries as well as the level of cooperation between them.

There are also plenty of email services operating out of the 14-Eyes countries,

including:

- **Tutanota (Germany)**
- **CounterMail (Sweden) (not open to new registrations)**
- **Posteo (Germany)**
- **Mailbox.org (Germany)**
- **StartMail (Netherlands)**
- **Runbox (Norway)**
- **Mailfence (Belgium)**

Harkening back to themes mentioned earlier in this article, Tutanota has been ordered by a regional court to implement encryption backdoors. The company is fighting several such requests at the moment.

*You may also like to read: The most secure email providers*

### Five Eyes encrypted messaging services: WhatsApp, Signal, Wickr

Similarly to emails, there aren't many encrypted messaging services based in Five Eyes countries. However, some of the most prominent ones are: WhatsApp is the most popular app in the category and it's owned by Facebook.

With what we know about the UKUSA Agreement, **this is a huge red flag because of PRISM**. According to the Snowden leaks, the NSA has a surveillance program to collect communications data from US tech companies, including Facebook (and therefore, WhatsApp as well).

## Surveillance systems of the Five Eyes alliance

The Five Eyes alliance operates various surveillance systems, some of which we know very little about. However, the media has discussed a few of these systems (or programs) quite a bit. For example:

- **ECHELON**. Probably the oldest Five Eyes surveillance system, with origins

**ECHELON**. Probably the oldest Five Eyes surveillance system, with origins in the Cold War. ECHELON was formally established in 1971 with the objective of monitoring military and diplomatic communications of the Soviet Union and its Eastern bloc allies during the Cold War.

- **PRISM**. One of the newer and more troubling Five Eyes surveillance systems, PRISM, was established in 2007. Its purpose is to collect communications data from large tech companies, including Microsoft, Yahoo!, Google, Facebook, and others.
- **XKeyscore**. Another relatively new Five Eyes system with the objective of internet surveillance. Edward Snowden paints XKeyscore as the be-all and end-all tracking system that lets the NSA read any online communication and know the location of any smart device.

## FAQ

### Why is it called Five Eyes?

The name of the alliance refers to the **5 main signatories of the UKUSA Agreement** – USA, UK, Canada, Australia, and New Zealand.

### How do I protect myself against mass surveillance?

To avoid mass surveillance, you should use software such as the best VPNs, password managers, encrypted email, and messaging tools. However, it's recommended to avoid cybersecurity services based in Five Eyes countries or other countries that don't respect their citizens' privacy.

### What countries are in the Five Eyes?

The Five Eyes countries are the US, the UK, Canada, Australia, and New Zealand.