Share

INSIGHT

US surveillance: s702 FISA, EO 12333, PRISM and UPSTREAM

Richard Lawne

13/08/2020

In Schrems II, the Court of Justice of the European Union ("**CJEU**") invalidated Privacy Shield based on the potential interference with data subject rights caused by US government surveillance carried out under Section 702 of FISA and EO 12333. The Court also referred to PRISM and UPSTREAM, two surveillance programs revealed by the Snowden leaks. You can read our reaction to the decision here.

This article provides a brief overview of the surveillance regimes referred to by the CJEU in its decision. It does not address all of the surveillance activities carried out by the US government or the laws that govern law enforcement requests (like the CLOUD Act).

Section 702 of FISA

The Foreign Intelligence Surveillance Act ("**FISA**") was enacted in 1978 to regulate US governmental electronic and physical surveillance of communications for foreign intelligence

purposes. It has been amended, strengthened and reformed a number of times, including by the USA Patriot Act of 2001, the FISA Amendments Act of 2008 and the USA FREEDOM Act of 2015.

FISA authorises government surveillance through various means: electronic surveillance, physical searches, pen register and trap and trace surveillance and business record searches. All FISA activities are overseen by the Foreign Intelligence Surveillance Court ("**FISC**"), which sits in a secure courtroom in Washington D.C. Decisions by the FISC may be appealed to the Foreign Intelligence Surveillance Court of Review ("**FISC-R**").

FISA was originally intended to govern surveillance activities targeting individuals inside the US. In 2008, however, s702 (50 USC §§ 1881a et seq) was enacted to authorise the acquisition of foreign intelligence information about **non-US persons located outside the US**. A non-US person is anyone who is not a US citizen or permanent US resident.

s702 reportedly provides the basis for more than a quarter of US international terrorism intelligence. Although targeted at non-US persons, it is also believed to result in the "incidental" collection of millions of Americans' communications. s702 essentially works as follows:

> Unlike the "traditional" FISA provisions, which require the government to obtain orders on an individualised basis and demonstrate probable cause, the Attorney General ("**AG**") and Director of National Intelligence ("**DNI**") submit **written certifications** to the FISC that jointly authorise surveillance activities for up to one year. The government does not have to specify which non-US persons will be targeted or demonstrate probable cause. It merely needs to attest that a significant purpose of the activities is to obtain foreign intelligence information and certify that appropriate targeting and minimisation procedures will be implemented.
>
> Once the FISC has approved a certification, the government issues directives to US **electronic communications service providers** that compel the providers to "immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition" of communications. In practice, the government sends the providers "selectors" (such as telephone numbers or email addresses) that are associated with specific "targets" (such as a non-US person or legal entity). Service providers must comply with these directives in secret and are not allowed to notify their users.
>
> The term "electronic communications service provider" is defined broadly to include **telecommunications carriers** (e.g., AT&T, T-Mobile, Verizon), providers of **electronic communications services** and **remote computing services** (e.g., Facebook, Google and AWS), as well as **any other communications service providers that have access to wire or electronic communications** (either in transit or in storage). According to guidance issued

by the Department of Justice, the definition is broad enough that it could potentially capture any company that provides its employees with corporate email or a similar ability to send and receive electronic communications, regardless of the company's primary business or function.

EO 12333

While FISA generally covers surveillance activities inside the US, the government may also conduct surveillance **outside the US** under the authority of Executive Order 12333 (EO 12333). In broad terms, EO 12333 provides the foundational authority by which US intelligence agencies collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means.

Unlike FISA, surveillance under EO 12333 does not rely on the compelled assistance of electronic communications service providers. The technical details remain classified and obscure, but the NSA has confirmed it involves **exploiting vulnerabilities in telecommunications infrastructure**.

There are controls around how US government agencies can obtain signals intelligence. In 2014, President Obama issued Presidential Policy Directive 28 (PPD-28) which directed US intelligence agencies to review their policies regarding the treatment of non-US persons in connection with signals intelligence programs. Effectively, PPD-28 imposes restrictions on signals intelligence activities, including those conducted under s702 FISA and EO 12333, regardless of the target's nationality or location. In Schrems II, the CJEU found that the protections afforded by PPD-28 are not sufficient to ensure an adequate level of protection under EU law.

PRISM and UPSTREAM

In 2013, Snowden leaked a number of NSA slides revealing the existence of two government surveillance programs: PRISM and UPSTREAM. Both are conducted under s702 of FISA but operate in different ways:

> PRISM involves the **direct 'downstream' collection of communications** by the NSA through the compelled assistance of electronic communications service providers. Effectively, the government sends a selector, such as an email address, to a US-based provider, and the provider is required to provide the government with all communications sent to or from that selector.

> As its name suggests, UPSTREAM involves the **indirect 'upstream' collection of communications** through the compelled assistance of **telecommunications providers that provide the backbone of the internet** (e.g. AT&T and Verizon). Essentially, the NSA copies and filters the vast quantity of data flowing through the network of cables, switches and routers that make up the Internet. Because the data is obtained **without the knowledge or assistance of downstream providers**, UPSTREAM has been described as a form of 'backdoor' surveillance.

Again, relatively little is known about how PRISM and UPSTREAM operate. The best source of information is a 2014 report by the Privacy and Civil Liberties Oversight Board, which played an important role in Schrems II – the CJEU's conclusions regarding US surveillance programs were based largely on the findings of the Irish High Court, which, in turn, drew heavily from the PCLOB report.

Legal challenges to Section 702 of FISA

There have been a number of lawsuits in the US challenging the legality of s702. The most notable are *Clapper v Amnesty International USA (2013) and Wikimedia Foundation v NSA (2020)*.

> In *Clapper*, a number of attorneys, journalists, and human rights organisations challenged s702 on the grounds it violates Article III and the First and Fourth Amendments of the US Constitution. The Supreme Court held, in a 5-4 decision, that the plaintiffs did not have Article III standing to seek relief under FISA. In essence, the plaintiffs failed to demonstrate that they had or would suffer injury as a result of s702, and they could not satisfy this requirement by merely claiming a reasonable likelihood that their communications would be intercepted.
>
> In *Wikimedia*, a similar claim was brought by a number of organisations, including Wikimedia (the parent company of Wikipedia). In 2015, the first eight plaintiffs were dismissed due to lack of Article III standing (following *Clapper*). Wikimedia was considered different to the other plaintiffs, on the basis that the sheer volume of its global communications made it virtually certain that the NSA had at some time intercepted, copied and reviewed its communications. In December 2019, however, Wikimedia's claim was also dismissed for lack of standing. In a deftly-executed motion, the government successfully demonstrated that there are technically feasible methods by which UPSTREAM could hypothetically operate without copying and reviewing Wikimedia's communications – while at the same time confirming nothing about how UPSTREAM actually operates. Wikimedia is appealing the decision.

Both cases show the extreme difficulties organisations face in challenging s702 without actual proof that their communications have been targeted or intercepted. This point also played an important role in Schrems II, because it evidences the difficulty non-US persons would have in obtaining legal redress in the US.

Transparency reports

In 2015, in response to the public outcry following the Snowden revelations, Congress enacted the USA FREEDOM Act. The Act mandates limited government reporting about FISC applications and authorises private companies to publish the numbers of FISA orders and other national security demands they receive (within certain bands).

> The **government reports** include those issued by the FISC, the Department of Justice and the Director of National Intelligence.
>
> There are a number of companies which publish their own **transparency reports**. These include Apple, AT&T, Facebook, Google, Microsoft, Twitter, Uber, Verizon and the Wikimedia Foundation.

Following Schrems II, it is likely that many other companies will follow suit.