Volume 15, Issue 3
cecileparkmedia.com

DATA PROTECTION LEADER

A **Cecile Park Media** publication | March 2018

The reauthorisation of Section 702 of FISA

Alex Berengaut and Jadzia Butler of Covington & Burling LLP break down what changed - and, perhaps more interestingly, what didn't - for FISA's reauthorised Section 702 programme, which will be in place for at least the next six years in the US.

Cover image: Ray Hennessy / Unsplash.com
Page 3 image: Bharath Suresh / Unsplash.com

CECILE PARK MEDIA

Editor Eduardo Ustaran
eduardo.ustaran@hoganlovells.com

Managing Editor Alexis Kateifides
alexis.kateifides@dataguidance.com

Editorial Assistants
Rachael Nelson-Daley, Cristina Ulessi, Kaveh Lahooti, Ellen O'Brien

Data Protection Leader is published monthly by Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND

Telephone +44 (0)20 7012 1380

Website cecileparkmedia.com

Eduardo Ustaran Partner
eduardo.ustaran@hoganlovells.com
Hogan Lovells International LLP, London

Editorial: Regulating internet data uses for good

This year, my book *The Future of Privacy* will become five years old. In it I argued how the use of data could, and should, be regulated to enable technological innovation and protect people's privacy at the same time. Today, this need is more real and urgent than ever. There is worldwide outrage at how our daily digital interactions are being tracked and manipulated for sinister purposes. Senior politicians and CEOs are getting involved in trying to sort out what is regarded as an indefensible invasion of our privacy at a global scale. But yet, whatever solutions are devised, they will need to be attuned to the reality we are all now used to: universal multimedia communications and the instantaneous availability of all human knowledge...for free. In other words, any approach that disregards this reality will surely fail to effectively safeguard the fundamental right to privacy and data protection.

Scandals tend to provoke knee-jerk reactions. And knee-jerk reactions hardly ever turn out to be good decisions. For that reason, we should look beyond the obvious and seek innovative solutions to what has become the most elusive riddle of our generation. For example, rather than blindly calling for all possible uses of personal information to be subject to individuals' consent, we should focus on making privacy by default work. In practice, privacy by default should involve considering the possible harmful effects that collecting, using or disclosing personal information may have and doing something to avoid them. This must be an ongoing and demonstrable duty for anyone tracking, profiling and targeting on the internet. However, to be successful, privacy by default should not mean the automatic end of these activities but undertaking them in an ethical and sustainable way.

This does not mean either that we should not be able to have control over our data. This is an underlying aim of data protection law which is fully compatible with the digital economy. The question is how to make use of the rights that exist in the law in a truly meaningful way. One approach that is encouraged by regulators and broadly accepted by the industry is the idea of privacy dashboards and granular privacy settings. But in reality, only a minority of people - although possibly a growing one - will actually ever make proper use of those tools. Therefore, we must develop innovative ways of not only allowing people to exercise a degree of control over their data, but also sharing with them the value derived from it. Would it be too much to expect that, as a rule of thumb, all users of personal information gave back a demonstrable benefit to the individuals to whom the information relates, unless there is a higher interest that should prevail, such as law enforcement or public safety? Just a thought.

On top of that, we seem to be missing a trick here. By far the most effective way of regulating the use of personal information is to prove that responsible exploitation brings benefits beyond avoiding a huge fine. Enforcement has an essential role to play of course, but for the vast majority of organisations, the motivation to do the right thing does not come from dodging a stick, but from the prospect of earning a big carrot. When dealing with privacy and data protection, that carrot is trust and a much greater effort is needed to show the bottom line benefits of generating genuine trust.

Today, the future of the internet as we know it looks grim. Those whose business models rely on collecting and analysing data or who aspire to develop such models are being accused and threatened with harsher than ever regulation. The rest of us - humble internet users - are facing the prospect of more annoying tick boxes or reduced services, or both. It need not be this way. Perhaps we, as consumers and citizens, should be paying greater attention to the uses made by others of our data in order to better protect ourselves, but the greatest emphasis of all should be on how to achieve responsible behaviours for everyone's benefit. Let's not get distracted by endless debates about the need or not for consent. Let's not pursue the routes that have shown to be unsuccessful in the past. Law and regulation exist for a reason, but they need to work. Existing privacy laws have powerful tools that need to be further explored and developed - from well-established principles like fairness and data minimisation to newer features like privacy by default and other practical accountability measures. Let's avoid the mistakes of the past by being more imaginative about the future.

Alex Berengaut Partner
aberengaut@cov.com

Jadzia Butler Associate
JButler@cov.com

Covington & Burling LLP, Washington DC

The reauthorisation of Section 702 of FISA

In 2008, Section 702 of the Foreign Intelligence Surveillance Act ('FISA') Amendments Act established a surveillance programme aimed at collecting foreign intelligence information from non-US persons located abroad. Having been renewed once in 2012 during the Obama Administration, the programme was scheduled to sunset on 31 December 2017 absent congressional reauthorisation. Several reforms were proposed during the reauthorisation process, but most were ultimately not adopted. In this article, Alex Berengaut and Jadzia Butler, Partner and Associate respectively at Covington & Burling LLP, break down what changed (and, perhaps more interestingly, what didn't) for the Section 702 programme, which will be in place for at least the next six years.

Background

Section 702 of FISA is the product of two surveillance programmes initiated by the Bush Administration following the attacks of 11 September 2001. The first programme, known as the Terrorist Surveillance Program, authorised the National Security Agency ('NSA') to collect certain international communications content without a warrant or other judicial court order. The second programme entailed using 'traditional' FISA Court ('FISC') orders to compel private, US-based service providers to assist in the acquisition of communications of individuals located overseas who were suspected of engaging in terrorism. Finding it impractical, and even impossible, to attain the requisite court order based on probable cause for each and every foreign target that the Government wanted to surveil, the Administration proposed modifications to FISA that spurred the Section 702 programme that exists today.

Under Section 702, the Attorney General and the Director of National Intelligence ('DNI') annually certify with the FISC proposed surveillance programmes that target non-US persons reasonably believed to be located abroad. The certifications must:

- identify the categories of foreign intelligence information sought;
- identify the targeting and minimisation procedures meant to ensure that US-person communications will not be inadvertently collected;
- attest that a 'significant purpose' of the programme is to obtain 'foreign intelligence information,' and;
- attest that the programme comports with the Fourth Amendment and FISA.

Unlike the preexisting, 'traditional' FISA, Section 702 does not require individual FISC authorisation for each individual target, or that the target be a suspected terrorist, spy, or other agent of a foreign power.

Calls for reform

In 2013, then-NSA contractor Edward Snowden disclosed the existence of the Section 702 surveillance programme and its various components to several media organisations. Numerous investigations into the scope and mechanics of the programme followed, including requests for additional disclosures from the Government, congressional hearings, and reports by the Privacy and Civil Liberties Oversight Board. With the programme's 31 December 2017 sunset date on the horizon, civil rights activists and several members of Congress (such as Ron Wyden, Rand Paul, Patrick Leahy, Steve Daines, and Elizabeth Warren in the Senate, and Representatives Zoe Lofgren, Ted Poe, Justin Amash, Beto O'Rourke and Thomas Massie in the House) sought to reform several aspects of Section 702.

Scope of collection and 'about' collection

Although Section 702 has been largely described as a national security programme focused on counter-terrorism, reform advocates have noted that FISA itself requires only that surveillance be geared towards collecting 'foreign intelligence information' more broadly (and even then, 'foreign intelligence' need only be a 'significant purpose' of Section 702 surveillance). As a result, some advocates have called for a tightening of the definition of 'foreign intelligence information' to make it more closely tied to national security and counter-terrorism.

Relatedly, US persons' communications are sometimes 'incidentally' acquired during 702 surveillance of non-US persons. For example, US persons' data may be swept up when they communicate with foreign targets, or because they reference a 702 target in the body of a communication (a surveillance practice known as 'about' collection). The NSA voluntarily ended the practice of 'about' collection in April 2017, but some advocates of reform suggested that a reauthorised 702 programme should categorically prohibit 'about' collection.

Querying and use of Americans' data for non-foreign intelligence purposes

Communications collected under Section 702 may be retained in databases at the NSA, the Central Intelligence Agency, and the Federal Bureau of Investigation ('FBI') for several years at a time. Although data collected under Section 702 is meant to be 'foreign intelligence information' belonging to 'non-US persons,' government agents can query databases containing 702 data for information about US persons, sometimes as part of routine criminal investigations. In addition, 702-acquired

In 2013, then-NSA contractor Edward Snowden disclosed the existence of the Section 702 surveillance programme and its various components to several media organisations.

information may be used against US persons in criminal court for certain serious crimes. This practice, referred to by critics as the 'backdoor search loophole,' was among the more controversial elements of the 702 programme during the reauthorisation debate. Some advocates, for example, proposed requiring the FBI to obtain a warrant before *querying* the 702 database for criminal evidence, while others proposed requiring a warrant to *access* any responsive content returned by a US-person query.

Transparency

Although the Government's declassification and transparency efforts have dramatically increased in recent years, some 702 reformers have argued that the surveillance programme's true scope and mechanics were too secret for the Government to be held accountable by the FISC, Congress, or the public. Several reform efforts therefore included calls for additional mandatory disclosures, such as annual estimates of the number of Americans whose communications have been collected, further declassification of FISC opinions, and the total number of times the Government has searched for Americans' information within 702 databases.

The reauthorisation bill

On 18 January 2018, Congress enacted legislation reauthorising Section 702, and on the 19th of January it was signed into law. The FISA Amendments Reauthorization Act of 2017 ('the Reauthorisation Act') generally did not enact the reform proposals under discussion. Specifically:

Congressional approval of 'about' collection

The Reauthorisation Act does not declare 'about' collection to be unlawful under the 702 surveillance programme. Instead, should the Government wish to end its voluntary cessation of the practice, the Reauthorisation Act requires the Attorney General and the DNI to submit their intention to Congressional Judiciary and Intelligence Committees for approval.

Limitations on access and use of Americans' data

The Reauthorisation Act does not require a warrant before querying 702 data for Americans' information. However, the Attorney General must now adopt querying procedures for 702 data. The Reauthorisation Act provides that these procedures must be consistent with the Fourth Amendment, and records of queries involving US persons must be retained.

In addition, the FBI is now required to obtain a court order before reviewing the results of queries unrelated to national security that use US-person search terms. However, no court order is needed if the FBI obtains a separate FISC order, or if the FBI independently determines that there is reason to believe that the results of a query 'could assist in mitigating or eliminating a threat to life or serious bodily harm.' Finally, the Reauthorisation Act prohibits using information obtained via Section 702 as evidence against a US person in any criminal proceeding, unless the FBI obtains a separate FISC order *or* the Attorney General independently determines that the criminal proceeding 'affects, involves, or is related to' national security or a variety of other types of criminal proceedings (including proceedings related to the Computer Fraud and Abuse Act of 1986 and transnational crime).

Additional transparency requirements

The Reauthorisation Act contains some additional required disclosures, but not the specific requirements that reform advocates sought. For example, the DNI is now required to release annual estimates of the number of times the FBI has opened a criminal investigation of a US person based 'wholly or in part' on foreign intelligence information gathered under Section 702. In addition, the Attorney General must submit to Congress an annual report of total subjects targeted (rounded to the nearest 500) and the number of such individuals who were US persons (rounded to the nearest *band* of 500, starting with 0-499).

Conclusion

Particularly given the substantial efforts to reform the 702 surveillance programme, the Reauthorisation Act is distinctive more for what it does *not* include than what it *does*. The revised 702 surveillance programme is now scheduled to sunset on 31 December 2023.