Data Protection in the United States

Catalyst.Net Limited (Catalyst)

Version 1.1

January 2018

Commercial in Confidence

catalyst
open source technologists

Level 6, Catalyst House, 150 Willis Street, Wellington 6011
PO Box 11053, Manners Street, Wellington 6142, New Zealand
+64 4 499 2267 // enquiries@catalyst.net.nz // www.catalyst.net.nz

Summary

1 Introduction

1.1 Under the domestic laws of the United States, the US Government can require individuals and organisations to provide it with data they own or can access. There is uncertainty around the scope of this power, the extent to which it applies to data processed or held outside of the United States, and to data held by non-US individuals and organisations.

1.2 This document outlines aspects of the relevant legal context, and then looks at a number of case studies to illustrate how some of the legal rules are applied in practice. The document concludes with the recommendation that individuals and organisations concerned with the protection of their personal data from unjustified interference by the US Government can mitigate these concerns by hosting their data outside of the United States, with a non-US hosting provider.

Legal Context

2 The USA Patriot Act

2.1 The USA Patriot Act (the Patriot Act) was signed into law by President George W. Bush in October 2001.[1] The Patriot Act gave sweeping new powers to the US government to obtain and collect data about individuals' and organisations' behaviour and digital communications.

2.2 Under the Patriot Act:

(a) Telecommunications providers could be required to hand over certain communications records, including, where appropriate, the details of session times and the durations of electronic communications, as well identifying information about the devices being used, like phone numbers and IP addresses.[2]

(b) The Federal Bureau of Investigation's (FBI's) powers to access telephone and transactional records held by telecommunications providers about their customers and employees were expanded.[3]

(c) The US Secret Service is empowered to investigate "computer fraud".[4]

(d) "Assistance" is provided to the Attorney General "to ensure that information derived from electronic surveillance or physical searches...is disseminated so it may be used efficiently and effectively for foreign intelligence purposes".[5] In addition, the heads of federal law enforcement

1 USA Patriot Act, P.L. 107-56 (2001).

2 Ibid, s 210.

3 Ibid, s 505.

4 Ibid, s 506. Richard Horowitz, Esq, *Summary of Key Sections of the USA Patriot Act of 2001* (http://www.rhesq.com/terrorism/patriot_act_summary.pdf).

5 Ibid, s 901.

agencies are required to disclose certain information obtained in the course of a criminal investigation to the Director of the Central Intelligence Agency (CIA).[6]

2.3 It was initially intended that some of the more controversial provisions of the Patriot Act would expire in December 2005. However, these provisions were extended until 2006, and then extended again in 2010. A day after their final expiry in 2015, the USA Freedom Act was enacted, which allowed for the continuation of mass surveillance and data collection practices.[7]

3 The Foreign Intelligence Surveillance Act

3.1 The Foreign Intelligence Surveillance Act (FISA) is a legislative regime that establishes principles and procedures for the surveillance of, and data collection from, individuals and organisations.[8] It establishes the FISA Court, which has the power to grant surveillance warrants to federal law enforcement and intelligence agencies. Surveillance warrants allow the relevant agency to access the data specified in the warrant.

3.2 The FISA Court's proceedings are conducted in secret – only the relevant government agency is present in a hearing on the application for a surveillance warrant. This has naturally led to accusations of bias against the Court,[9] which are perhaps not unreasonable given that between the FISA Court's inception in 1979 and 2013 it had granted 35,434 applications for electronic surveillance warrants, and declined only 12.[10]

4 Other Legislation and Rules

4.1 There are a number of other laws that allow the US Government to access individuals' and organisations' data. The Stored Communications Act (SCA) allows the US Government to compel ISPs and other third-party telecommunications providers to hand over customers' data where certain requirements are met.[11] For data that is 180 or fewer days old or, a warrant is required. For certain data that has been stored for more than 180 days, prior notice and an easily obtainable administrative subpoena are sufficient.[12]

4.2 In addition, Rule 41 of the Federal Rules of Criminal Procedure allows the FBI to obtain a "hacking warrant" permitting it to access data held on any computer in the world, in certain circumstances.[13]

6 Ibid, s 905.

7 USA Freedom Act, P.L.114-23 (2015).

8 Foreign Intelligence Surveillance Act, P.L. 95-511, (1978).

9 See for example: The Guardian, *FISA Chief Judge Defends Integrity of Court over Verizon Records Collection*, June 2013, https://www.theguardian.com/world/2013/jun/06/fisa-court-judge-verizon-records-surveillance.

10 EPIC, *Foreign Intelligence Surveillance Act Court Orders 1979-2016*, 2016, https://epic.org/privacy/surveillance/fisa/stats/default.html.

11 Stored Communications Act, 18 USC Chapter 121, ss 2701-2712.

12 Emden Law, *Stored Communications Act: The Good, the Bad and the Ugly*, September 2015, https://www.emdenlaw.com/stored-communications-act-the-good-the-bad-and-the-ugly/.

13 F.R. Crim. P., rule 41.

Practical Context

5 The NSA-Verizon Scandal

5.1 In 2013, it was discovered that the FISA Court had issued a warrant to the National Security Agency (NSA) requiring a subsidiary of the largest telecommunications provider in the United States to supply the agency with a daily feed of "telephony metadata" about all of its customers.[14] This data included comprehensive call records, text messages and location data.

6 Extraterritoriality: *Microsoft Corporation v United States*

6.1 In the same year, a New York court issued a warrant under the SCA requiring Microsoft to hand over all emails and other information associated with a particular Microsoft account.[15] Microsoft refused to produce the bulk of this information, arguing that the SCA was not intended to have extraterritorial application, and that it should not be required to hand over the information because it was stored on servers located outside of the United States. After a lengthy court process, this argument was eventually accepted by the US Court of Appeals (Second Circuit).

6.2 While this case could be viewed as a victory for the protection of data against excessive government interference, it should be noted that the decision is only binding within the Second Circuit (that is, the states of New York, Connecticut and Vermont). In addition, the US Department of Justice (along with 33 states) has appealed the decision to the US Supreme Court, which will determine the final outcome during its 2017-2018 term. Given the current conservative majority on that court, a reversal of the Court of Appeals' decision is distinctly possible.

6.3 Outside of the Second Circuit, other companies – including Google – have adopted a practice of complying with search warrants directed at data held on overseas servers, according to the US Justice Department.[16] This has resulted in the fairly unsatisfactory position that whether or not data hosted with a US hosting provider overseas will be disclosed to the US government under a search warrant depends on the identity of the hosting provider, and the location of the court which issued the warrant. The inconsistency of federal law on this issue increases the likelihood that the Supreme Court will agree to review the *Microsoft* case.

6.4 Significantly, there is a bill currently before the US Congress that would allow "a government entity to require providers of electronic communication services or remote computing services to disclose the contents of communications in electronic storage (e.g. the cloud) regardless of where those communications are located".[17]

---

14 The Guardian, *Verizon Forced to Hand Over Telephone Data – Full Court Ruling*, June 2013, https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

15 See: Microsoft Corporation v United States 829 F.3d 197 (2d Cir. 2016).

16 Ars Technica UK, *Google Stops Challenging Most US Warrants for Data on Overseas Servers*, November 2017 (https://arstechnica.co.uk/tech-policy/2017/09/google-stops-challenging-us-warrants-overseas-servers/).

17 Congress.Gov, *S.2986 – International Communications Privacy Act*, November 2017 (https://www.congress.gov/bill/114th-congress/senate-bill/2986).

7 The DreamHost Warrant

7.1 In July 2017, a US Court issued a search warrant against DreamHost, a company that provides web hosting services, requiring it to disclose information relating to a website used to organise protests at the inauguration of US President Donald Trump. The information to be disclosed included "over 1.3 million IP addresses – in addition to contact information, email content, and photos of thousands of people – in an effort to determine who simply visited the website".[18]

7.2 DreamHost asked for clarification around the scope of the warrant, and the US Department of Justice's response was to file a motion to compel compliance with it. This motion was challenged by DreamHost, and, following negative media coverage, the Department of Justice narrowed the scope of its request. While the warrant was eventually upheld, its scope was furthered narrowed so that identifying information of people not participating in criminal activity would not be disclosed.

Conclusion

8 Recommendations

8.1 There are real and increasing risks to the integrity, security, and privacy of data held by US-based providers of hosting services, including Microsoft, Google, Amazon and others. The powers of the US Government to conduct mass surveillance and to access individuals' and organisations' private data are expansive, and have been steadily increased over the last twenty years. This trend of expansion is likely to continue under the Trump administration. An Executive Order issued in January 2017 directs agencies of the US Government to "...ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information".[19]

8.2 It is significant to note that even though cases such as *Microsoft v United States* appear to suggest a willingness on the part of US courts to reign in illegitimate attempts to gain access to users' data, it would likely be prohibitively expensive for all but the largest organisations to challenge such attempts in court.[20]

8.3 As a general rule, the US Government does not have jurisdiction over individuals and organisations who are outside of the United States and have no citizenship or residency connection to the United States. Therefore, an effective way to mitigate the risk of unjustified interference with data is for that data to be:

(a) hosted outside of the United States; and

(b) hosted with a non-US hosting provider.

18 DreamHost, *We Fight for the Users*, August 2017 (https://www.dreamhost.com/blog/we-fight-for-the-users/).

19 White House, *Executive Order: Enhancing Public Safety in the Interior of the United States*, January 2017, (https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united).

20 This is particularly significant in the US context, because, unlike in many other counties, successful litigants in US courts do not receive a contribution to their legal costs from the losing party as a general rule. As noted above, even large corporations like Google have shown a reluctance to challenge these warrants.

It is not sufficient that data merely be hosted outside of the United States, because despite the *Microsoft* case, other US courts have been willing to uphold warrants for the effective seizure of data hosted outside of the United States by US hosting providers.[21] By hosting data with a non-US provider in a privacy-friendly jurisdiction, individuals and organisations concerned with data protection can achieve a significant reduction in the risk of undue interference by the US Government.

21 See: *In re Search Warrant No. 16-960-M-01 to Google* (3 February 2017).