Exercising Jurisdiction Over Foreign Corporations: The USA PATRIOT Act and the Extent to Which US Government Law Enforcement Agencies Can Obtain Information from Abroad

Ken Wong considers the implications of the PATRIOT Act on the ability of US Government law enforcement agencies to obtain information from abroad.

Introduction

Almost 13 years ago, the then US President George Bush signed into law the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (***PATRIOT Act***). Ever since, the PATRIOT Act has been at the centre of controversy in the international community in relation to its impact on the privacy of individuals. Prior to the signing of the PATRIOT Act, certain law enforcement and intelligence gathering legislation already had well-established extraterritorial effect. But the effect of the PATRIOT Act was to increase that extraterritorial scope. Whether data is stored within the walls of a building or in the cloud, US courts have exercised jurisdiction over foreign corporations in order to compel the production of information for the purposes of US law enforcement.

if a non-US corporation has 'continuous and systematic' contacts with a US corporation, it may be subject to US jurisdiction

The first section of this article identifies the powers which are available to US law enforcement agencies to obtain information under current US legislation. The second section highlights how the US courts have exercised jurisdiction over foreign corporations before the PATRIOT Act was signed into law. The third section is a short case note on the recent Microsoft challenge in respect of a search warrant which compelled the production of information held by its Irish subsidiary.[1] The case highlights how the US District Court applied relevant legislation after the PATRIOT Act was enacted. Finally, this article briefly discusses some considerations which may be relevant to Australian organisations when contemplating engaging with contractors and cloud computing providers.

The various methods by which US law enforcement agencies can obtain information

There are several methods available to US law enforcement agencies to obtain information from US entities and foreign companies subject to US jurisdiction. These tools were strengthened by the PATRIOT Act, which was enacted as a legal response to the terrorist attacks on 11 September 2001.[2] The PATRIOT Act amended a suite of laws relevant to law enforcement and intelligence gathering. Its preamble states that it is an 'Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes'.[3]

Foreign Intelligence Surveillance Act (***FISA***)

FISA is the key item of legislation that was amended by the PATRIOT Act. The kinds of documents that can be obtained by the Federal Bureau of Investigation (***FBI***) are now significantly broader and include anything that is tangible as well as electronic data.[4] Recipients of a FISA order may not disclose the existence of, or the details relating to, such order.[5] One of the most significant changes was the lowering of the legal threshold for FISA orders such that the FBI need only 'specify that the records concerned are sought for an authorised investigation... to protect against international terrorism or clandestine intelligence activities'.[6] This means that a FISA order can be issued to a company which is not itself the subject of an investigation.[7]

National Security Letter (***NSL***)

NSLs enable the FBI to request various business records for the purposes of national security. An NSL is an administrative subpoena issued by the agency instead of by the court.[8] The kinds of information available to the FBI are primarily business related, which may include financial, credit, telephone and internet activity records, but content information is excluded.[9] Similar to the expansion of the scope of FISA, the PATRIOT Act also expanded the scope of NSLs. As well as imposing non-disclosure obligations, the legal threshold was also significantly reduced to only show that the information sought is relevant to a national security investigation.[10]

Grand jury subpoena

Subpoenas may be issued through *ex parte* proceedings involving a grand jury comprising a group of 16 to 23 civilian jurors to investigate the existence of possible criminal conduct .[11] Grand juries base their investigations on mere suspicion and do not follow the rules of evidence.[12] Their investigatory powers are substantial and virtually any person or document can be the subject of a grand

1 *Re Matter of a Warrant* 13 Mag. 2814 (2014).

2 Department of Justice, *The USA Patriot Act: Preserving Life and Liberty*, <http://www.justice.gov/archive/ll/highlights.htm>.

3 Department of Justice, *Text of the Patriot Act* <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>.

4 Patriot Act of 2001 § 215.

5 Ibid.

6 Ibid.

7 P Swire, *The System of Foreign Intelligence Surveillance Law*, 72 Geo. Wash. L . Rev. 1306, 1329 .

8 J Billings, *European Protectionism in Cloud Computing: Addressing Concerns Over the PATRIOT Act*, (2012) 21 CommLaw Conspectus 211, 216 .

9 18 USC §§ 2709 and 3414.

10 Patriot Act of 2001 § 505.

11 M Geist and M Homsi, *Outsourcing Our Privacy?: Privacy and Security in a Borderless Commercial World,* (2005) 54 UNBLJ 272, 279.

12 Ibid.

jury subpoena.[13] The PATRIOT Act amended the Federal Rules of Criminal Procedure with respect to grand juries to permit the production of documents in relation to 'matters occurring before the grand jury' involving 'foreign intelligence or counter intelligence' to 'any Federal law enforcement, intelligence, protective, immigration, national defence or national security official in order to assist the official receiving that information in the performance of his official duties'.[14]

Search warrant

Search warrants are issued by a court exercising jurisdiction over the investigation. US law enforcement agencies are required to follow the Federal Rules of Criminal Procedure and must be able to show probable cause.[15] Probable cause could be a reasonable belief that a person the subject of the investigation has committed, is committing, or is about to commit, a crime.[16] Contents of email communications and other non-content related information may be obtained by a search warrant issued under § 2703(a) of *Title 18 of the United States Code* (***18 USC***). The *Stored Communications Act* (***SCA***) was codified by 18 USC and was enacted as part of the *Electronic Communications Privacy Act of 1986*. The PATRIOT Act amended § 2703 of 18 USC to provide for nationwide service of search warrants for electronic evidence.[17]

Mutual legal assistance treaty (***MLAT***)

These are bilateral agreements under which the US Government and the foreign country to which it is a party cooperate to obtain information from each other for the investigation of crime by either country. Australia is a party to an MLAT with the US.[18]

The extraterritorially of US legislation before the PATRIOT Act

Prior to the signing of the PATRIOT Act, certain US law enforcement and intelligence gathering legislation already had well-established extraterritorial effect. This section of the article highlights how the US courts have exercised jurisdiction over foreign corporations before the PATRIOT Act was enacted.

If a foreign corporation has a connection with a US corporation, a test that the US courts have used to determine whether that foreign corporation is subject to US jurisdiction is the 'minimum contacts' test.[19] That is, if a non-US corporation has 'continuous and systematic' contacts with a US corporation, it may be subject to US jurisdiction.[20] Furthermore, when a US corporation is served with an order to produce data that is in its in possession, custody or control, and such data is held by a foreign related entity, the US courts will have regard to the closeness of the relationship between the entities to determine the level of control over the data.[21]

Where the relationship is between a US parent company and a foreign subsidiary, the US courts have considered the extent of control the US parent company has over its foreign subsidiary. The relevant test for control is whether the parent company has direct or indirect power through another company or series of companies to elect a majority of the directors of another company.[22] If the parent company has the requisite power, it will be deemed to be in control of the other company.[23]

While it is likely that a foreign subsidiary of a US parent company would be subject to US jurisdiction, there has been one case where it was held that a foreign parent company was subject to US jurisdiction. In the case of *Re Grand Jury Proceedings the Bank of Nova Scotia*,[24] which concerned the service of a grand jury subpoena on the Bank of Nova Scotia's US subsidiary branch for the production of financial information held in the Bahamas and Cayman Islands, the court held that the Canadian parent company is not excused from '[performing] a diligent search upon receipt of the trial court's order of enforcement' even if it resulted in possible breaches of local Bahamas and Cayman Island secrecy laws.[25]

Whether the services comprise data storage at a data centre or the provision of hosted software, performing due diligence on the cloud provider and understanding where the location(s) of data will be stored is vital

In another case, one US court has shown that extraterritoriality applied in the context of a tax investigation by the Internal Revenue Service. In the case of *United States v Toyota Motor Corp*,[26] summonses were issued to the Japanese parent company and to its US subsidiary. At first instance, the court found that it had personal jurisdiction over the Japanese parent company because the US subsidiary was considered a managing agent of its parent company as that term is used in the Federal Rule of Civil Procedure. The court concluded that the information sought was required to be produced because it was 'necessary for a fair and accurate determination of Toyota USA's tax liability'.[27]

Microsoft's unsuccessful challenge

With the exception of MLATs, each of the powers available to US law enforcement agencies identified above have been expanded by the PATRIOT Act. This section of the article examines how a US District Court recently applied the expanded legislation under

13 Ibid.

14 Patriot Act of 2001 § 203.

15 N Fossoul, *Does the USA Patriot Act Give U.S. Government Access to E.U. Citizens' Personal Data Stored in the Cloud in Violation of the E.U. Law?*, (2012) Paper for Tilberg University LLM Law & Technology, 14.

16 Ibid.

17 Patriot Act of 2001 § 108 .

18 *Mutual Assistance in Criminal Matters (United States of America) Regulations 1999.*

19 *International Shoe v Washington* 326 U.S. 310 (1945).

20 *Goodyear Dunlop Tires Operations, S.A. v Brown*, 131 S. Ct. 2846, 2851 (2011).

21 J Billings, above n 8, 217.

22 *In Re Investigation of World Arrangements* , 13 F.R.D 280 (D.D.C. 1952).

23 Ibid.

24 740 F.2d 817 (1984).

25 Ibid, 88.

26 569 F. Supp 1158 (C.D. Cal 1983).

27 Ibid, 5.

which a search warrant was obtained. In *Re Matter of a Warrant*,[28] the District Court of the Southern District of New York considered a motion by Microsoft Corporation (***Microsoft***) to quash a search warrant issued to it on the grounds that the US Government is not authorised to issue search warrants for extraterritorial search and seizure.

Facts

Microsoft operates and provides web-based email services under various domain names which include 'hotmail.com', 'msn.com' and 'outlook.com'. Email messages sent and received by its users are stored in Microsoft's data centres which exist in multiple locations both domestically and internationally. The location where the data is stored depends on the proximity of the user to the closest data centre.

On 4 December 2013, Francis J issued a search warrant which authorised the search and seizure of information associated with a certain email account 'stored at premises owned, maintained, controlled or operated by Microsoft'.[29] Microsoft complied with the search warrant to the extent that the relevant information was stored in servers in the US, however, it refused to comply in relation to other relevant information because it was stored in servers in Dublin, Ireland.

The relevant test for control is whether the parent company has direct or indirect power through another company or series of companies to elect a majority of the directors of another company

Microsoft subsequently filed a motion to quash the search warrant to the extent that it required the production of information that was held in Ireland.

The search warrant

The judge discussed extensively the nature and extraterritorial operation of the search warrant since the scope was expanded by the PATRIOT Act. The search warrant was obtained under § 2703(a) of 18 USC, which enables the US Government to seek from internet service providers such as Microsoft unopened emails stored by the provider for less than 180 days, as well as the kinds of information that would be available under a subpoena issued under § 2703(b) of 18 USC and under a court order issued under § 2703(d) of 18 USC.[30]

This is a very wide and powerful instrument and can compel the production of:

- basic customer information, such as the customer's name, address, internet protocol connection records, and means of payment for the account;
- content of opened emails regardless of age and content of unopened emails that are more than 180 days old; and
- historical logs showing the email addresses with which the [user] had communicated.

The judge's decision and reasoning

The judge rejected Microsoft's argument that the US Government is not authorised to issue a search warrant to the extent that it required the production of information held outside of the US. In his reasoning, the judge considered the nature of the search warrant, the legislative history of the SCA, and the practical consequences that would flow from adopting Microsoft's argument.

The judge found that the nature of the search warrant was such that it was a hybrid order which consists of part search warrant and part subpoena. Although the procedure by which it is obtained and the showing of probable cause were prerequisites to obtaining a search warrant, in terms of its execution, the order was akin to a subpoena in that it was served like a subpoena and the search and seizure of information did not require physical access to premises by US Government agents.[31] The judge's importing of the subpoena-like characteristics into the search warrant meant that the law of subpoenas applied and the recipient was required to produce the requested information which was in its possession, custody or control regardless of the location of that information.[32]

The judge also considered the legislative history of the SCA and the objectives of the relevant PATRIOT Act amendments to the SCA. Prior to the amendment, a search warrant could only be obtained in the district in which the evidence is located.[33] He considered the policy rationale underlying § 108 of the PATRIOT Act and cited that the amended § 2703(a) 'attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet... [and such] time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned'.[34] Since the PATRIOT Act has now provided for nationwide service of search warrants, US law enforcement agencies are now able to obtain a search warrant from a court with jurisdiction over the investigation without requiring the intervention of its counterpart in the district in which the internet service provider is located.[35]

The judge also considered the practical implications that would flow if a § 2703(a) search warrant was territorially restricted. He concluded that it is unlikely that Congress intended to treat a § 2703(a) order as a conventional search warrant that involves a physical search of premises in which the evidence is located. He reasoned that a § 2703(a) order could not be a conventional search warrant because if it were, it could only be executed abroad which required the intervention of a foreign country through an MLAT.[36] The judge concluded that Congress' intention of giving § 2703(a) orders the extraterritorial reach meant that the 'slow and laborious MLAT process and the risk that the government of the other country may not prioritise the case as highly' was able to be bypassed.[37]

Microsoft is intending to appeal the decision.[38]

---

28 13 Mag. 2814 (2014).

29 Ibid, 3.

30 Ibid, 8.

31 *Re Matter of a Warrant*, above n 28, 12.

32 Ibid.

33 Ibid, 17.

34 Ibid.

35 Ibid.

36 Ibid, 21.

37 Ibid, 19.

38 Microsoft News, *Federal Judge Rules Against Microsoft In Overseas Search Warrant Case,* < http://microsoft-news.com/federal-judge-rules-against-microsoft-in-overseas-search-warrant-case/>.

Some considerations for Australian organisations

Australian organisations contemplating engaging contractors need to consider the risk of information falling into the hands of the US Government. In some cases, this could occur without their knowledge. Therefore, performing due diligence on the contractor is critical.

Before entering into an agreement with a contractor, careful consideration needs to be given to the extent to which data will be disclosed to the contractor. In particular, it is important to consider whether the data will only be held in Australia and whether there is a likelihood that data will be disclosed to an overseas entity. In a scenario where a contractor is a wholly Australian entity operating only in Australia, restricting the right of subcontracting and including a privacy clause in the contract mitigates that risk.[39] If the agreement permits subcontracting, however, it may be necessary to have the ability to approve subcontractors.[40] The level of risk will be far greater if a proposed subcontractor operates in, or has a connection with, the US.

If a contractor is an Australian entity that is part of a multinational group with a US parent company, it is likely that the Australian contractor will be subject to US jurisdicton and the risk of producing data to the US Government pursuant to an order is high. However, such risk may be somewhat reduced by preventing the flow of data to the US parent of the contractor.[41] Customers should therefore include a clause which provides for such. A useful alternative could be an obligation on the part of the contractor not to delegate any of the contracted services to any US related entity.

Australian organisations contemplating contracting with a cloud computing provider need to also consider the risks of storing data in the cloud. The risks of storing data with a non-US cloud provider that is a subsidiary of a US parent corporation is high because that provider is likely to be subject to US jurisdiction. The risks of storing data with a US cloud provider is even higher. These risks invariably raise concerns for data privacy and confidentiality for Australian organisations that have procured, or that are contemplating procuring, cloud computing services. Whether the services comprise data storage at a data centre or the provision of hosted software, performing due diligence on the cloud provider and understanding where the location(s) of data will be stored is vital. This is because the laws of the country in which the data is located is likely to have jurisdiction.

Conclusion

There is a real risk that Australian data might be the subject of a US order for production. This risk could be mitigated by ensuring that technical and contractual measures are in place before engaging with contractors or cloud computing providers. Whether a US court can exercise jurisdiction over an Australian corporation will depend on the extent of any connection with a US corporation. If an Australian corporation is a subsidiary of a US parent corporation, it is likely that a US court could exercise jurisdiction over the Australian corporation. With the rising popularity of cloud computing, the risk is exacerbated if there is a lack of control and visibility of the flow of data between data centres locally and abroad.

If an Australian corporation is a subsidiary of a US parent corporation, it is likely that a US court could exercise jurisdiction over the Australian corporation

Ken Wong is a Corporate Solicitor at Toyota Finance Australia Limited.

---

39 Treasury Board of Canada Secretariat, *Guidance Document: Taking Privacy into Account Before Making Contracting Decisions* <http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp00-eng.asp>.

40 Ibid.

41 Ibid.