Freshfields Bruckhaus Deringer

The long arm of the USA Patriot Act: tips for Australian businesses selecting data service providers.

Connie Carnabuci, Partner

November 2011

WHAT IS THE BIG ISSUE?

U.S. authorities may exercise extraterritorial powers against non-U.S. entities to obtain non-U.S. data if the data is stored on a server located in the U.S., or controlled by or in the possession of a U.S. company, under the USA Patriot Act. It is not a defence for a U.S. company that possesses or processes data to say that it does so outside the United States.

The availability of access to data without a warrant and the broad powers available under the Patriot Act have no parallel in Australian law. This analysis provides an informed view of the risks for Australian businesses associated with storing your data with U.S.-owned or U.S.-linked data service providers, and the advantages of storing your data with service providers that are not connected with U.S. entities and that will store your data, and your customer's data, outside the U.S. and outside of the ambit of the Patriot Act.

WHAT IS THE USA PATRIOT ACT?

In the aftermath of September 11, 2001, the United States enacted the Patriot Act to facilitate foreign intelligence and international terrorism investigations. While the intended focus of the Patriot Act is on terrorist activities, its provisions have broadly enhanced the ability of the U.S. government to collect documents and data within and outside the U.S., even where the link to terrorism is remote or speculative.

The U.S. government can obtain disclosure of data in the custody or under the control of any company or data centre with sufficient connections to the U.S. such as U.S. companies operating foreign subsidiaries outside the U.S., foreign companies operating subsidiaries in the U.S., foreign subsidiaries with a U.S. parent company, and their data service providers around the world.

Apart from making it easier to obtain a court order for production of customer and customer transaction information, the Patriot Act has given the U.S. government highly intrusive informal means of obtaining such information, such as National Security Letters ("NSLs"). Whilst in theory judicial review of such government actions is available, in fact, to date, such review has been limited. After the passage of the Patriot Act, the number of NSL requests issued by the FBI has increased dramatically. The FBI issued approximately 39,000 requests in 2003, approximately 56,000 requests in 2004, approximately 47,000 requests in 2005, and approximately 49,000 requests in 2006. In 2006, the overwhelming majority of requests sought access to electronic records.

Even where no formal Patriot Act subpoena has been served, U.S. companies have eagerly shared information with the U.S. government when the government based its request on national security grounds. For example, the three largest U.S. telecommunications companies – AT&T, Verizon, and BellSouth – provided the phone records of tens of millions of Americans to the National Security Agency ("NSA") even though the NSA never obtained a warrant for any of the information. Similarly, AT&T, Verizon, and MCI turned over an undocumented number of phone records to the FBI starting in the period immediately following September 11, 2001. Although the companies claimed to have acted pursuant to NSLs issued under the

Freshfields Bruckhaus Deringer

ABOUT FRESHFIELDS BRUCKHAUS DERINGER

Freshfields Bruckhaus Deringer is a global firm with more than 470 partners and over 2,500 lawyers around the world. We have offices in China and other countries in Asia, Europe, the Middle East, and the United States and have worked with clients on their transactions in almost every country in the world. In jurisdictions where we do not currently have an office, we maintain excellent relationships with the leading law firms and work with them regularly.

customers, the vendor may be legally prohibited from notifying their customers of the subpoena."

Conclusion

Sourcing data services from an Australian subsidiary of a U.S. service provider, or a local provider who stores data on a server in the U.S. will mean that your data and your customer's data will be subject to the long arm of the Patriot Act. The Patriot Act extends far beyond the borders of the United States and can compel disclosure of data stored outside the U.S. even where disclosure would violate the laws of the country where the data was located. While blocking statutes may potentially be used to prevent such compelled disclosures, there are no reports to date of blocking statutes which have successfully prevented the U.S. government from accessing data stored with companies and data centres outside the U.S. where U.S. national security is concerned. As such, foreign companies and data service providers with connections to the U.S., either through a U.S. parent or a U.S. subsidiary, cannot prevent compelled data disclosure by the U.S government invoking the Patriot Act.

Customers should therefore consider the security and confidentiality risks posed by the Patriot Act and related U.S. discovery laws, and consider storing their data with companies and data service providers which do not have any U.S. connections, when selecting a service provider. The power of the Patriot Act to access data stored outside the United States is certainly not just a theoretical risk.

Patriot Act, a U.S. Department of Justice audit concluded that, in many instances, the FBI had not in fact issued an NSL.

As an Australian company can the U.S. government really compel disclosure of my data?

Yes. Even prior to the passage of the Patriot Act, U.S. courts required U.S. companies to turn over data located overseas, including data held by non-U.S. subsidiaries and affiliates, where the U.S. entity had possession, custody or control of the data in question. In a law enforcement context, U.S. courts have been particularly aggressive in compelling production of non-U.S. data and have required compliance with U.S. subpoenas even where disclosure of the materials violated the laws of the country where the data was located. If a data centre is located in Australia but owned or operated by a U.S. entity, data stored in that centre could be accessed under a Patriot Act request even if such a request would violate Australia's National Privacy Principles.

Recent activity in Canada provides a very real focus of how such issues may play out.

In May 2004, in the context of considering public sector outsourcing arrangements, the Office of the Information and Privacy Commissioner for British Columbia ("OPIC") sought submissions on the implications the Patriot Act has on the privacy of British Columbians. Based on more than 500 submissions from Canada, the U.S. and Europe, the OPIC issued a report entitled "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing" which stated that there was a reasonable possibility that a FISA court could order production of documents and data that are within the custody or control of a U.S. company, such as a U.S. parent company with access to records held by its Canadian subsidiary and data service provider. The report stated that, as a practical implication of the Patriot Act, individuals and entities seeking to store their data in the global cloud may be deterred from dealing with businesses that share their data or that of their customers with U.S.-linked companies, including their subsidiaries, affiliates and data service providers whether within or outside the U.S.

In October 2005, the OPIC ruled that an organisation with a presence in Canada like the Canadian Imperial Bank of Commerce ("CIBC") that outsources the processing of personal information to a U.S. firm cannot on the basis of its offshore location prevent its customers' personal information from being lawfully accessed by U.S. authorities operating under the Patriot Act even where such access conflicts with Canadian privacy laws. In this case, the Assistant Commissioner found that because CIBC required its customers to share their personal information with CIBC's U.S.-based company as a condition of service, there was sufficient connection between CIBC and its U.S.-based company for the FISA court to exert jurisdiction over CIBC even though the company and its data are located outside the U.S.

Again in May 2006, the OPIC determined that where an organisation has established a presence in Canada but shares its customers' personal information with its U.S.-based parent, U.S. authorities pursuant to the Patriot Act may still compel the Canada-based subsidiary to disclose any data stored in its cloud without obtaining the consent of its customers. In such circumstances, foreign subsidiaries outside the U.S. cannot protect

its customers' personal information from being lawfully accessed by U.S. authorities. The Assistant Commissioner noted that "while customer personal information is in the hands of a foreign third-party service provider, it is subject to the laws of [the foreign] country and no contract or contractual provision can override those laws." Canadian privacy laws cannot protect data located in Canada from the Patriot Act in those circumstances.

HOW DO SERVICE PROVIDERS WITH A U.S. PARENT COMPANY RESPOND TO THIS ISSUE?

At a JAWS-User Group summit held on March 4, 2011, Ojima Hideki, Amazon Data Services Japan KK's managing director, admitted that "because Amazon is a U.S. company, the data centre of Amazon Web Services in Tokyo will fall within the scope of the USA Patriot Act".

During the launch of Microsoft Office 365 in June 2011, Gordon Frazer, Microsoft UK's managing director, similarly acknowledged that, as a U.S.-headquartered company, all data stored on a Microsoft server, irrespective of where that server is located, is subject to the Patriot Act's provisions. When asked whether Microsoft could guarantee that its EU-stored data would never leave the continent, Mr. Frazer replied: "Microsoft cannot provide those guarantees. Neither can any other company." Since its headquarters are in the U.S., it is obligated to comply with U.S. laws, including the Patriot Act.

In August 2011, Google became the next major company to admit that any data stored on its server, whether the server is located within or outside the U.S., is also subject to the Patriot Act's provisions. In a formal statement issued on August 16, 2011, Google's spokesperson confirmed that, "as a law abiding company, we comply with valid legal process, and that – as for any U.S.-based company – means the data stored outside of the U.S. may be subject to lawful access by the U.S. government." This admission from Google was made in response to the report issued by the German media group, WirtschaftsWoche, that Google has received and complied with numerous requests from the U.S. intelligence agencies to disclose data stored in its European data centres on account of U.S. national security.

WHAT IS THE REACTION IN THE INTERNATIONAL COMMUNITY TO THIS ISSUE?

Governments around the world have taken steps to protect their citizens from the threat posed by the Patriot Act to the confidentiality of cross border IT/data services. For example, the Netherlands has excluded U.S. cloud providers from bidding on government IT contracts because of concerns over the Patriot Act's extraterritorial reach. In a written answer to a parliamentary question relating to U.S. cloud companies storing Dutch data and the impact of the Patriot Act, Dutch Minister Ivo Opstelten commented that any contract with a U.S. cloud provider would have to include terms restricting the provider from moving the data outside of the European Union which "basically means that companies from the United States are excluded in such bids and contracts".

Also in response to the confidentiality and privacy risks posed by the Patriot Act, the Canadian government has instructed its departments to refrain from using computers

in the global network that are operating in the U.S. According to a 2006 report released by the Privacy Commissioner of Alberta entitled "Public Sector Outsourcing and Risks to Privacy", Commissioner Frank Work urged public bodies that maintain population-wide information systems carrying sensitive personal information to keep such personal information within Canadian borders to ensure that it doesn't fall into the wrong hands. Whilst such an approach would not escape the reach of the Patriot Act if the Canadian data centre was owned or otherwise linked to the U.S., it serves to illustrate that foreign governments have in recent years been looking for ways to try to protect their citizens' right to privacy and mitigate risks associated with the Patriot Act.

Similarly, Deutsche Telekom AG's T-Systems IT has recently announced that it is in discussions with the Federal Office of Information Security ("BSI") to influence European regulators to forge a certification system that would allow German cloud operators to protect their data storage against intervention by the U.S. government. If implemented, the certification system would allow German cloud providers having no connections to the U.S. to market their cloud services and products by indicating to customers and consumers that the BSI has certified that they are not subject to the scope of the Patriot Act.

Members of the European Parliament have also condemned the breadth of the Patriot Act and described recent further amendments to U.S. discovery laws as a "real threat to European data". As confusion over the Patriot Act and how it applies to IT services continue to shroud the European Union in controversy and uncertainty, the European Union has proposed to amend the Data Protection Directive and is currently in discussions to improve the current international data handling provisions.

WHAT IS THE REACTION IN AUSTRALIA TO THIS ISSUE?

In April 2011, the Department of Finance and Deregulation in Australia issued a paper entitled, "Cloud Computing Strategic Direction Paper: Opportunities and applicability for use by the Australian Government", which specifically references the Patriot Act when highlighting the potential risks associated with cloud computing. The paper states that Australian government agencies need to be aware of legislative and regulatory requirements, such as the Patriot Act, in other geographic regions as compliance may be a challenge for the agencies. The paper does not, however, acknowledge the fact that the Patriot Act might well apply to Australian data centres owned by or linked to U.S. entities.

In the same month, the Department of Defence also issued a paper entitled, "Cloud Computing Security Considerations", in which the Defence Signals Directorate ("DSD") recommends Australian agencies to refrain from outsourcing information technology services and functions outside of Australia, unless the agencies are dealing with data that is all publicly available. According to the paper, the DSD "strongly encourages agencies to choose either a locally owned vendor or a foreign owned vendor that is located in Australia and stores, processes and manages sensitive data only within Australian borders," because foreign owned vendors operating in Australia may be subject to foreign laws such as a foreign government's lawful access to data held by the vendor." Moreover, even "if the vendor is subpoenaed by a foreign law enforcement agency for access to data belonging to the vendor's