US Patriot Act: Implications For Outsourcing to US Companies

David Chan considers the *'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001'* and the potential for personal information in the possession of a US outsource provider to be disclosed to the FBI.

Recent announcements by the governments of South Australia and British Columbia that each is reviewing the effect of US anti-terrorism laws on their outsourcing policies highlights the difficulty that arises when local privacy obligations conflict with information gathering by government agencies.

The specific concern is that a US corporation with activities in a foreign country (say Australia) may be required, under the *US Patriot Act*1, to disclose personal information that is in its possession. This is of more immediate concern as in recent years large US corporations such as EDS and IBM have been providing much of our governments' IT infrastructure. For example, EDS currently handles the tax records of the Australian Taxation Office and most of South Australia's State government systems.

OUTSOURCING AND LAW ENFORCEMENT

The onward march of the digital age inevitably results in more and more personal information being stored "on-line" (actually on computer servers located elsewhere), and it's no surprise that law enforcement agencies have sought access to this vast information resource on grounds of national security. The growth of information technology outsourcing as a business strategy means that a government agency's files will now mostly be stored on servers owned by third party IT companies, just as the ISPs may outsource their storage to operators of server warehouses. Law enforcement agencies have consistently sought access to these third party systems but have until recently been restrained by a combination of civil libertarian persuasiveness and just plain old inertia. The events of September 11, 2001 overcame this inertia and in the US, the *US Patriot Act*, which was passed swiftly following the events of September 11, has given law enforcement agencies what they have long sought.

THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Amid provisions which enhanced the powers available to US law enforcement agencies, the *US Patriot Act* also amended the *Foreign Intelligence Surveillance Act (US) 1978 Act* ("***FISA***"). The *FISA* is the act that gives US law enforcement agencies the power to access personal information. Prior to 1995 warrants were limited to electronic surveillance (e.g. wire taps) but in 1995 this was expanded to include the seizure of "certain records"2 (i.e. without the need for any surveillance).

The *FISA* also established a secret court, the Foreign Intelligence Surveillance Court, where law agencies are able to obtain orders giving them access to personal and private information. Section 1861(d) of the *FISA* makes it an offence for a person to even disclose to another person that personal information was sought or obtained by a law enforcement agency. As a result, the extent to which these activities are being carried out is almost impossible to ascertain.

Prior to the *FISA*, in order to obtain a warrant to compel access to personal information, the US enforcement agencies had to show that there was some evidence of wrongdoing. The *US Patriot Act* amendments to the *FISA* significantly relaxed this test. While section 215 of the *US Patriot Act* amended the *FISA* to allow US agencies to obtain records to protect against international terrorism and against clandestine intelligence activities, it also relaxed the test for obtaining a warrant. Whereas previously an applicant for such warrant had to show evidence giving reason to believe that the person whose records are sought is capable of being a foreign agent, now they only have to show that records are sought for the purpose of an authorised investigation into foreign intelligence not concerning someone who is a US citizen. Section 218 of the *US Patriot Act* further amends the *FISA* to relax the requirement that foreign intelligence gathering be the sole purpose for obtaining information. It now only has to be a "significant purpose".

Accordingly, a US law enforcement agency, such as the FBI, could obtain an order from the Foreign Intelligence Surveillance Court to compel a US company with operations in Australia to disclose information that it holds in its possession, so long as foreign intelligence gathering is a *significant purpose* for obtaining such information. It hardly seems that law enforcement agencies were

overly restricted by the sole purpose test. Between 1979 and 2001, the FISA Court approved all but 5 of more than 14,000 requests for warrants to compel access to personal information.3

IMPLICATIONS FOR OUTSOURCING

The *US Patriot Act* has much greater international implications when one considers that most of the major IT firms which are capable of large-scale infrastructure services are US- based. IBM, EDS, and HP account for more than 40% of the market for enterprise IT outsourcing.4

IBM and EDS are understandably adamant that the personal information they acquire pursuant to outsourcing contracts is secure5. EDS points to the privacy provisions in its contracts, which it says are designed to protect the security of the individual's information, and the application of the *Privacy Act* to that information. According to a spokesperson for the company, if the US Government wanted Australian information for law enforcement purposes, EDS would take up the matter with the Australian authorities6.

The report by the Privacy Commissioner of British Columbia makes it clear that it would regard a disclosure of information by a US company of British Columbian personal information to be an offence under their local privacy legislation7.

In Australia, personal information is protected by the *Privacy Act*8. National Privacy Principle ("NPP") 2.1(e)9 provides for the primary duty of an organisation not to disclose personal information to a third party, unless it reasonably believes that such disclosure will lessen or prevent a serious threat to public safety. Note 1 of NPP 2 specifically provides that the non-disclosure principle is not designed to deter law enforcement agencies from performing their function. It is unclear whether disclosure to a foreign law enforcement agency in order to lessen or prevent a serious threat to public safety, in Australia or elsewhere, falls within the scope of the exception.

NPP 9 provides that personal information may be transferred to a foreign country only if the organisation providing it reasonably believes that the recipient of the information is subject to a law which upholds principles for fair handling of information that are substantially similar to the NPPs. Even though the US is governed by its own federal privacy legislation10, the personal information, if handed to the US, would be governed by the *US Patriot Act*.

The US companies in Australia insist that they abide by the laws of the country in which they operate11. IBM recently stated that no personal information has in fact been disclosed by the company pursuant to the amended *FISA*12. Undoubtedly, commercial considerations act as a powerful incentive not to disclose personal information, and it is no surprise to hear the US companies loudly trumpeting their devotion to non-disclosure. However, it would not be too cynical to suggest that, if faced with considerable legal and political pressure from the US government, such devotion may be severely tested, and avenues of permitted disclosure explored. Significantly, if such information were obtained from the US companies in Australia under *FISA*, section 1861(d) would preclude the companies from disclosing this fact to any person. In addition, section 1861(e) relieves those who in good faith provide personal information to the FBI under an order from the

FISA Court from any liability to any other person for such production.

A further cause for concern is that the *US Patriot Act* eliminates the barrier between national security surveillance and US local law enforcement. The fear is not just that personal information may be disclosed to US law enforcement agencies in the course of anti-terrorism investigations, but that the information obtained may be used by US authorities to bring criminal charges against people for all manner of offences. A decision by the highly secretive Foreign Surveillance Review Court confirmed that the FBI now has much more latitude to share information obtained through national security surveillance with local US criminal law enforcement agencies13.

WHAT CAN BE DONE?

Privacy advocates have recommended new legislation to make it an offence to disclose information under the circumstances envisaged in the *FISA*, supported by sanctions against the individuals concerned. In the current climate, this does not appear to be likely, especially in Australia where the federal government has unreservedly supported the US government's anti-terrorism laws and 'war on terror' generally, and has strengthened our own laws accordingly.

Australian organisations concerned with the security of the personal information which they acquire may need to follow the example of the South Australian and British Columbian governments in reviewing their outsourcing arrangements and policies. One answer would be to cease outsourcing IT operations to companies subject to the jurisdiction of the *FISA*, or simply to cease outsourcing at all. In any proposed outsourcing agreement between a holder of personal information and a company subject to *FISA* jurisdiction, it may be prudent to consider including an express prohibition on disclosures under foreign laws such as *FISA*, except where expressly required or permitted by Australian court order, and the contractual remedies for such disclosure, regardless of whether made in accordance with the laws of the foreign country. Of course, detecting a breach, and enforcing a remedy, remains problematic in light of section 1861(d).

David Chan is the General Manager of Argo Lawyers in Sydney and has worked in the IT and legal industries for over 10 years.

1 USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001)

2 For an extensive review of FISA, see Elizabeth B. Bazan, *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions* (CRS Report for Congress, 2003); the report is available on the website of the Federation of American Scientists: www.fas.org.

3 Stephen J. Schulhofer, "No Checks, No Balances: Discarding Bedrock Constitutional Principles" in Richard C. Leone and Greg Anrig Jr., eds., *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* (New York: Public Affairs, 2003) 74 at 81.

4 www.gartner.com

5 Hayes, Simon, "US law raises privacy worries", *The Australian* (2 November 2004)

6 Ibid.

7 British Columbia. Office of the Information and Privacy Commissioner. Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing.

8 1988 (Cth)

9 Schedule 3 *Privacy Act 1998 (Cth)*

10 US Privacy Act 1974

11 Supra Note 5

12 Ibid.

13 *In Re Sealed Case* 310 F.3d717 (Foreign Intelligence Surv. Ct. Rev 2002)