Submission No 151

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Juliette Vrakas

RESPONSE TO
EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS
DICUSSION PAPER JULY 2012
Submission lodged on 20 August 2012
By Juliette Vrakas

Introduction

There are existing security vulnerabilities within industry participants (telecommunication providers) which have taken their labour offshore into the control of foreign state powers. A large vacuum has been created which assists criminals as well as espionage elements to infiltrate and compromise information about Australians. Telecommunication interception reforms, telecommunication sector security reform, and Australian intelligence community legislation reform cannot be strategic unless it considers the matters raised in this paper. The support and directions of the Australian Defence forces is imperative with all respect. The significant security vulnerability which has been created by new technologies has damaged the privacy of civilians and government on a global scale. Julian Assange has demonstrated to the world the existing vulnerabilities that can impact the future telecommunications initiatives and relations between state powers. The alleged theft of Australian identity to instigate covert operations and assassinations by foreign state powers is also a serious concern. Recently half a million citizens were affected by credit card theft, and millions of dollars compromised under the noses of government politicians and their ineffective security legislations. Australians are now vulnerable to all kinds of threats, including invasion of their privacy.

There is evidence of government inability to protect the private information of its citizens, by allowing telecommunications service providers to operate offshore , and permitting foreign access to Australian personal information which include details of citizens; full name, birth, residence, credit banking details, emails, and other affiliated private sector accounts. All without prior knowledge or initial consent by the Australian individual. Australian's are forced to accept the new technologies which have been created and imported even though they pose high security risks to their safety and wellbeing.

Australians no longer have control over voice recordings every time they make a telephone enquire about their accounts. They are forced to make legal agreements by answering mechanism using finger tips. The legal implications that can occur because of misuse of these technologies are a dangerous roulette for the safety of the Australian population. Because there is no control as to how their information is shared between institutions and individuals. The government is obligated to strengthen the safeguards and privacy of Australians. This must include exclusion of foreigners to access Australian data and citizen information. The national security has failed in their efforts to protect citizen information. Telecommunication provider and carriers hire foreign workers , for instance ; India, Malaysia, United States, and countries in the Asia region to access personal information about Australian.

Observations conducted over a span of a decade towards telecommunication providers and their policies; indicate that Australians have not been aware that their personal information has been disclosed to foreigners offshore. This has created a security risk, and has taken away the rights of Australian's to protect their private information. For millions of Australian's their identity has been released to foreign workers and espionage elements without their knowledge and informed consent. The failure by Australian government to protect citizenship privacy rights should be addressed in these security reforms. Whilst the government is expressing their views to expand their interception activities, it gives little concern to the vulnerabilities which exists to Australian information that is taken offshore into foreign countries. Foreign entities also have the capabilities to illegally intercept and obtain information from Australian businesses. It is highly unlikely that the amendments to the Telecommunication Act can address the security and resilience risks which are posed in this respect. One way to protect Australians and their personal information is to create a law which empowers the Australian citizen and allowing them to control use of their personal information. This includes having the right to restrict disclosure of personal information to limited government agencies. The government has failed to afford Australian's this opportunity (10).

Chapter One - Terms of Reference – Inquiry into Potential Reforms of National Legislation

It may be very well to amend ASIO's powers on warrant provisions with the use of their computers and communications , however these kinds of warrants that will be reviewed does not address the vulnerabilities that exist by telecommunication providers that are Australian owned or part owned whilst their computers are stored offshore (11). The increase in trends for offshore business operation is a major issue, and failure of politicians, warrants the Australian Defence Forces to take necessary actions to safeguard their citizens. When applying reforms to homeland security, the required amendments to the Intelligence Services Act must address a parallel reform to the offshore implications of Australian or part owned Australian telecommunication businesses operations (11).

Chapter Two - Interception and the TIA Act

There are no provisions in the TIA Act that adequately protect citizen information. There should not be any exception, the purpose of civilisation and citizenship is to protect the rights of its citizens, this incudes their identity, and privacy. Particular well known telecommunications organizations publically display their policy to include the Privacy Act 1988 and Part 13 of the Telecommunications Act. However the legislation has failed the Australian community in protecting their identity from offshore espionage elements, or foreign workers that currently have access to the private lives of Australians at overseas telecommunication posts. Telecommunication company policies which are publically made available do not address these security vulnerabilities that exist. The average Australian is now forced with little or no option to open telecommunication accounts with businesses that are privately owned and operate offshore. Posing a real security risk to their personal information. There is no legislation that permits citizens to prohibit these telecommunication industries from recording private information from an offshore base.

It may very well be that interception of telecommunication content and data is cost effective tool for law enforcement, but it is a large price for any Australian to pay when their information is compromised by offshore business operations that cannot be properly regulated by Australian full force of law (12). Privacy statements made by telecommunication providers does not guarantee that the data held in foreign states can protect the personal information it holds from misuse , or unauthorized access by foreign source. Interception techniques should include in this respect a DOB IN LINE made available, where unauthorized use, recordings or access be reported immediately to the

Australian government. Providing immediate channel for legal investigation and action to continue. The government is well to review the need for new interception regime, but it will fail in its investigation on offshore based Australian businesses, because it does not have the legal channel to control information that is stored in the territory of another state power. It may be well for government to address matters such as reducing the number of agencies eligible to access communications information; however it should consider permanent bans on all offshore based telecommunications operations that are susceptible to foreign invasion. If bans are not implemented than the reducing the number of agencies eligible to access communications information will be useless and a waste of public money (13).

It may be very well to implement offences for failing to assist in the decryption of communications, but how can this be applied to offshore business operation which are controlled by the foreign state powers, and may clash with Australian legislation? (13) It is evident with the government desires reform , but it should not be more concerned with establishing a channel to access mass information. It must not shift away from its duties to its people and that is to keep them safe and protect their identity. Therefore the government objective in this respect is concerned more on intelligence gathering rather than long term goals of protecting personal information from landing in criminal hands. It seems that this trend may be global, however does not make it right. If Australian's are made to feel more vulnerable and unsafe in their home country, the consequences in the near future will reveal serious threats in society that can no longer be contained. Solely because the technologies that currently exists in communications around the globe is capable of monitoring every citizens movements and activities by criminals and foreign espionage elements.

Transnational organized crime is running rapid because of the new technologies that are made available by state powers. The adoption of new telecommunications and technology has created the ability for foreigners to easily access Australia information. It is to some degree frightening, because the problem posed here, is that organized crime is indirectly aided by government. Consumer behaviour in the telecommunications industry is the responsibility of government. However there is a high risk factor in this modern age, that privatisation of the telecommunications industry means creating an unsafe world for its citizens (21).

Chapter Three - Telecommunications Security Sector Reform

2.1 Australia's telecommunications industry

The Governments Discussion Paper of July 2012 has ignored offshore Australian telecommunication industry security risks. The growing trend of Australian businesses being taken offshore is compromising Australian national security (30). Section 581 to the Telecommunications Act should not be the only power to cease supply of carriage service if the service would be prejudicial to security. The Australian Defence Force laws should be part of the telecommunications reform process. The Australian Defence Force is a traditional trained institution that knows the value of security to our nation. They must remain as a major participant in the telecommunication interception reforms, and security of Australians and their identity. The Telecommunication Act will not protect Australian's from criminal and foreign activities that exist on and offshore. The Governments Discussion Paper of July 2012 stated that the TIA Act does not address supply chain risks, software and hardware vulnerabilities or security risks to the telecommunications infrastructure. In particular concerns for example, the rising interest of facial recognition software and implications of authorizing its availability in the community (32). Science is getting out of control, and security is now lost in the maize of technological advancement for the sake of entrepreneurs and the elites.

2.4 Analysis

Co-operation between various sectors in the community including intelligence, security, defence trained personnel, academics, ordinary people that care about their home land and their families have the ability to understand the seriousness of these telecommunication issues. Encouraging participation of discussion papers to the community in Australia is a positive step for homeland security reforms. There are many citizens keen to assist the government in protecting the interests of Australia. The government must be constantly challenged in this respect.

3. Proposed approach

Regulatory framework to address the national security risks will fail because of the way the provisions are enacted in legislation. The provision to empower delegated individuals to make decisions that are not evidentiary based, and biased is a serious flaw to the regulative systems in Australia. Regulative frameworks will not deter any criminal organization or

foreign force from illegally accessing information or data offshore or onshore (33). Regulative institutions cannot control Australian offshore businesses operations. Regulative frameworks are increasingly becoming a form of suppression and damaging towards the integrity of innocent citizens and community and are abusive in nature. There requires serious reforms in the way decision makers construct decisions, in particular, how investigations are conducted. Decision makers must be made more accountable and be penalised for giving false and misleading statements which damages the reputation of businesses and individuals. This kind of suppression can be a precursor to more crime, because the regulative systems are too controlling, and the human experience will be unable to withstand so many conditions in the foreseeable future.

3.2 Compliance frameworks

Subcontracting maintenance and services to foreign owned or foreign based businesses is a real security risk. Many Australian telecommunication account holders are subjected to foreign entities accessing their personal information. Australia has failed to protect is citizens from this vulnerability. The government has not provided its citizen's access to Australian government owned telecommunications enterprises at the first instance. Therefore the government should conduct investigations on the current breaches of privacy which currently exist within the telecommunication industry to date.

3.3 Directions and penalties

Enforcement measures should be considered, however it is useless if the government continues to allows telecommunications business to operate overseas. Directions and penalties are unworkable if it allows aliens to access Australian data and information (38).

Chapter Four – Australian Intelligence Community Legislation Reform

2.1 Modernise the streamline ASIO's warrant provisions

Globalisation has created a trend where Australian businesses are moving offshore. The Australian government has not acted to stop this insecure trend. It may be well to modernise and streamline the ASIO's warrant provisions onshore, but will have nil affect to the telecommunication businesses operating offshore that have foreign interests. Computer access warrants will have nil affect to the computers based offshore. Listening and tracking device warrants and powers to inspect delivery service articles to offshore based businesses

where information about Australians are recorded will have nil affect. Other legislation comes into play here and reform would need to be addressed in this respect (41).

ASIO's national security concern is no longer national, it should span to the international level to an extent. Its powers should be the same if not equal to ASIS and other similar institutions. The modern world has forced local and national interest to include international interests. Perhaps a new institution to tackle this will be required such as "Australian Communication Security Force", which may incorporate both ASIO and ASIS or other similar bodies for example. The measures that are proposed to enhance the intelligence gathering capabilities should not compromise the security of Australians personal information. The major problem in this respect is the increase of offshore businesses operations that have provided easy access to the private lives of Australians.

In conclusion, this paper has touched briefly on the issues raised in the Government Discussion Paper of July 2012. It is not an exhaustive response, but merely strives to support the efforts for reform from a particular perspective. Telecommunication industry requires to be publically owned by the Australian Government where it can be managed, controlled and monitored efficiently. It is a new age where privatisation of the telecommunications industry creates more vulnerabilities and serious threats to our citizens and nation. Therefore my recommendations are as follows;

- Create a task force to investigate the matters raised about offshore telecommunications operations and the disclosure of citizen information to foreign entities.
- ban all telecommunication carriers and providers that do not have the full force of Australian law , and that are not Australian owned , and /or on Australian Territory
- Prohibit all telecommunication industries from hiring offshore foreign workers to access the millions of Australians personal information.
- Prohibit all telecommunication operators from accessing citizen information at any offshore foreign base.
- Strengthen the privacy of Australian information, by banning all voice and audio recordings that are currently operating at many institutions that are not Australian

owned , and that have foreign connections. Including the banning of voice recording and facial recognition in the private sector.

- Create new laws that require telecommunication providers, carriers to inform the Australian government if their information is likely to be taken offshore and accessed by foreign entities.
- Create a DOB IN LINE for Australians to raise their concerns about the way telecommunication businesses are operating and disclosing private information.
- The Defence Force to become a major participant in telecommunications reforms
- Australian government to be a major stake holder, and controlling force for all telecommunication businesses in Australia. Restrict the privatisation of telecommunication industry to Australians with no offshore business interests.

Reference:

Australian Government, *Equipping Australia Against Emerging and Evolving Threat*s, A Discussion paper to accompany consideration by the Parliamentary Joint Committee on Intelligence and Security of a package of national security ideas compromising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform, Attorney – General's Department.

END