Submission to Privacy Commission

April 10, 2014

Office of the Australian Information Commissioner

Government of Australia

Thank you for inviting public submissions.

Privacy is an inherent right of everyone. Invasion of privacy could have serious consequences in our lives. Democratic governments have the responsibility to protect the privacy of a person.

Often dictatorships and authoritarian rulers do not respect the personal privacy of its citizens. Countries with governments that do not have to answer to its people rule in any manner without respecting its citizens.

Dictatorships and authoritarian style rulers often conduct covert surveillance on its citizens to identify dissent against the rulers so that identified persons can be punished. The information obtained from subterfuge surveillance is analysed to formulate strategies for offensive pro government propaganda.

Invasion of privacy is prevalent in third world countries with corrupt governments. Many such governments are run by dictators who got to power by force, coercion or tainted elections.

Invasion of privacy leads to public disclosure of confidential personal information. Such information includes, residential address, date of birth, ethnic origin, marital status, religious affiliation, political propensity, sexual orientation, professional identity etc. Personal information may also include specialised skills, financial information, family background, views on social issues, academic information, names and details of spouse, siblings, parents, friends and colleagues. Personal information are sought out by criminal gangs for profit motives and for commercial benefits.

At the time of writing this submission, there is a heated argument going on between those who favour and are opposed to invasion of privacy versus protection of national security. Media tend to over simplify it by suggesting that the public has the right to know and then contradict it with the suggestion that those who are responsible for invasion of privacy must be punished to the full extent of the law.

In Australia Listening Devices Act, prevents unauthorised interception and/or recording of private conversation between two parties by a third party with the use of any technical aid. Any evidence produced from such interception is not only considered illegal and therefore inadmissible in any Australian courts, the offence carries imprisonment if it was found that a person’s privacy was deliberately and wilfully violated.

Privacy provision under Australian Federal Telecommunications Act stipulates that any illegal interception and recording of phone conversation by a third party is punishable.

Law enforcement agencies are required to obtain interception warrants from an appropriate court through the state or federal Director of Public Prosecution. Warrants for interception issued by all Australian courts have minimum validity period. Anyone found to have used an expired warrant to conduct wiretap surveillance on phone, on a premises or on a person, will be found guilty of offence and it is punishable.

Warrants for audio, video surveillance are only issued when it can be proven that the case is a matter of national security, economic security and/or part of serious criminal investigation and such evidence is significant and Judges make decision on an individual case merit basis.

Personal information gathered by all government agencies including intelligence agencies and law enforcement are bound to be protected by the collectors under the privacy laws in Australia. Any leakage of information is considered a criminal offence under Australian Criminal Code.

Australian commercial retail banks are bound by privacy laws with regard to financial information disclosure of account holders. Violation of privacy could result in action from banking regulatory authority. Credit reporting agency is bound by privacy law to protect credit information of its members and any breach of privacy is punishable.

In the United States federal law prohibits illegal interception and/or recording of third party conversations. Any audio/video surveillance require warrant issued from a court. Any such warrants issued must meet the threshold to satisfy a court that issuing such order was warranted due the seriousness of the case. Additionally convincing evidence has to be presented to the warrant issuing authority that the case had the merit to have such an order issued.

Personal information collected by all government agencies in the United States are required to comply with privacy laws. Any breach of privacy is punishable and the punishment is serious if the person that committed the offence is a government employee. Similar privacy rules apply to banks, credit reporting agencies and health service providers.

Privacy laws are even stricter in the United Kingdom where breach of privacy is considered a far more serious offence.

In summary maintaining strict privacy standards is an integral component in evidencing a thriving democracy with respect to the rights of its citizens.

With that said, protecting our privacy has become increasingly challenging due to internet, social engineering by unscrupulous criminal gangsters, cyber espionage, media probes etc.

Whilst we must protect privacy, we are also required to maintain press freedom to ensure a pluralistic democracy. Cyber espionage does not directly invade personal privacy however personal information leak is a collateral damage from cyber espionage. It’s the internet and social media engineering and social engineering in general that are the real culprits that commit invasion of privacy.

Protecting the privacy of private individuals must continue to remain an important point of focus for Australian government. Respect for personal privacy and information is a necessary proof of a functioning society that up holds democratic values.

At the time of writing this submission, I am a final year student doing Master in Information Security and Intelligence.

Please direct your comments and questions to me Joel Krose, at [redacted].