THOUGHTWORKS AUSTRALIA SUBMISSION TO SENATE LEGAL AND CONSTITUTIONAL COMMITTEE INQUIRY INTO THE TELECOMMUNICATIONS INTERCEPTION AND ACCESS ACT

About ThoughtWorks

ThoughtWorks Australia is a custom software development firm employing over 200 people in Australia. We are part of a worldwide firm of some 2400 people in 12 countries. We build business software including websites, mobile applications, and complex solutions. We also provide IT consulting services for many leading organisations in Australia and the world.

At ThoughtWorks, we have witnessed first-hand the adverse effects of the interception of data from Internet transmissions and data centres by the National Security Agency (NSA) and its counterparts, including the Australian Signals Directorate (ASD). We have been involved in many conversations concerning the future of our industry and the impact on individual privacy should this unauthorised blanket surveillance be continued.

Our colleagues in the USA have supported legislation before the US Congress to end the bulk collection of phone records, install a special advocate in the US surveillance court, and increase transparency for government agencies and online service providers.

Background

Given the AUSCANNZUKUS or "Five Eyes" agreement, the alleged participation of the ASD in the NSA's activities, and recent revelations of ASD's aggressive violation of the privacy of Australians, we believe many of the lessons learned and legislative changes proposed in the USA are pertinent to telecommunications interception and access practices in Australia.

ASD works directly with the NSA in mass surveillance activities in four joint facilities in Australia; at the US Australia Joint Defence Facility at Pine Gap and three ASD facilities: the Shoal Bay Receiving Station near Darwin, the Australian Defence Satellite Communications Facility at Geraldton, and the naval communication station HMAS Harman outside Canberra. [1]

And material revealed in the material being released by whistleblower Edward Snowden clearly shows the ASD has been carrying out for years the same kind of mass surveillance techniques that the NSA has, directed not only against the mass of the Australian population[2] but also against foreign government leaders, leading to the recent diplomatic crisis with Indonesia.

There is clearly no public mandate for the Australian government engaging in dragnet mass surveillance. 80% of Australians disapprove of Australian government agencies being able to access their telephone and Internet records without a warrant, while only 16% approve. [3]

---

[1] http://www.smh.com.au/world/snowden-reveals-australias-links-to-us-spy-web-20130708-2plyg.html

[2] http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

[3] http://essentialvision.com.au/documents/essential_report_140218.pdf

Urgent Need for Reform in a New Technological Environment

The context and pretext for this inquiry is the general failure of oversight mechanisms and legislation to keep up with technology development that enables extensive information collection and storage for later use. The Internet has evolved significantly over the last ten years with the growing popularity of mobile devices and social media. A huge amount of personal and sensitive information is transmitted constantly over the Internet. Mass surveillance without proper oversight is a significant invasion into personal privacy that affects everyone.

The Telecommunications Interception and Access Act ("TIA Act"), amended more than 45 times since September 2001, requires an overhaul to bring it into the digital age, to properly integrate Australia's National Privacy Principles, and to uphold our obligations under international human rights law.

Warrantless Access and Need for More Oversight

The TIA Act currently permits Australian agencies working outside law enforcement, such as CentreLink, to access data without a warrant. In 2011-12, personal information was accessed 293,501 times, which translates to 1 in 75 Australians if each were on a single individual. ThoughtWorks Australia believes that the number of agencies that can access this data needs to be confined to only those truly undertaking law enforcement and national security activities. We also believe that more rigorous oversight is required to access telecommunications data: judicial oversight and the need to obtain a warrant.

Metadata and the Practice of Data Austerity

"The Australian intelligence agency, then known as the Defence Signals Directorate (DSD), indicated it could share bulk material without some of the privacy restraints imposed by other countries, such as Canada.

'DSD can share bulk, unselected, unminimised metadata as long as there is no intent to target an Australian national,' notes from an intelligence conference say. 'Unintentional collection is not viewed as a significant issue.'"[4]

It would be misleading in the extreme to minimise the significance of what can be learned through metadata. As technologists, we know that metadata is not trivial either in the quantity or quality of information contained. Metadata could include information about telephone calls made, emails sent, information accessed online, or the location of mobile telephones. This information can be used to deduce very intimate details about a person's associations, interests and activities. For example, one wouldn't need to hear the conversation to make deductions about a phone call between a private individual and a divorce lawyer, or a cancer clinic, or a journalist.

ThoughtWorks believes that companies and governments should avoid storing large amounts of unnecessary personal data because of the vulnerability of that data to theft or misuse. Our latest "Technology Radar" publication discusses the German term "datensparsamkeit", which means "data reduction" or "data austerity". This describes the practice of storing only data that is necessary, rather than collecting everything that might be useful. Germany has evolved laws, such as the Federal Data

[4] http://www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

Protection Act (2009), which embrace the principle of data minimisation and data reduction, not least due to former regimes that have carried out extensive mass surveillance programmes.

Standard operating procedures that apply 'datensparsamkeit' require agencies or companies to determine not only why certain data is being captured and stored, but also what comprises the minimum required data. The burden is on companies and governments, at least in theory, to demonstrate a need for the data they store. They must make the case for sharing their data, rather than routinely collecting and storing it for policing, intelligence, or commerce. For example, "datensparsamkeit" recognises that an IP address is very revealing and not necessary to count hits on a website. It also recognises that some data is private; storing it poses risks to the rights of freedom of expression and association.

Adverse Impact on Business and Economy

There are many legal, moral, and civil liberties arguments against untargeted surveillance and the collection of metadata. As part of a global technology business, we have an additional motivation. Mass surveillance, including that which is undertaken under the current provisions of the TIA, is bad for business and the economy.

Some studies predict that the NSA's PRISM program could reduce revenues of US cloud computing industries by 20% — $35 billion — because customers want their data stored in less-surveilled countries. A Forrester Research paper puts that cost at $45 billion, adding domestic consumers opting for overseas providers. The Cloud Security Alliance found that 10% of foreign companies *had already cancelled* a project for cloud services with a US-based provider. Cisco, maker of routers at the core of Internet traffic around the globe, faces declines of 18-30% in orders in its top five emerging markets. IBM, Microsoft, and HP are also experiencing significant losses in emerging markets.

Australian businesses are vulnerable to similar trends if Australians' confidence in using the Internet to conduct private conversations and secure financial transactions falters. An overhauled TIA Act would play an essential role in providing clearer safeguards and oversight to increase consumer confidence.

Our clients are rapidly becoming digital businesses, relying on a thriving Internet and mobile network, both to support delivery of their products and services, and to engage with their customers and partners. Across industries — from entertainment to retail to media to software-as-a-service — the productivity and efficiency gains due to the growth of the Internet have not only unleashed unprecedented innovation in new types of products and services, but also the ability to deliver them globally.
Many of our clients are in the social sector. The Internet benefits them by massively amplifying their ability to engage with their target constituencies. It is their essential tool for organising, fundraising, monitoring healthcare in resource-poor environments, and crisis response. We also work in the education sector, where the ability to store and share knowledge is disrupting and transforming the way we learn by creating global communities of learners.

Adverse Impact on Personal Life, and Protection of Personal Privacy

We believe that the world works better when the Internet works better. The Internet, and its most ubiquitous application, the World Wide Web, present unprecedented efficiency in all aspects of business and personal life. The Internet provides near-instant communication by email, instant messaging, phone calls, and two-way interactive video calls — all at near zero marginal cost. The ability of citizens to participate freely in civil society using the World Wide Web has strengthened democracy worldwide.

The Internet changes markets. Through disintermediation, removing the broker between parties that want to transact with or learn from each other, it has dramatically changed industry after industry: travel, auctions, bookselling, music, advertising and news. And in doing so, it has drastically reduced costs and disrupted previously-dominant agents, replacing them with new ones. As with any disruption, there have been winners and losers. However, prices have declined, sales volumes have increased, and profits have gone up. Society as a whole is financially much better off. The Internet represents an $8-trillion-a-year economy, growing at an annual rate of roughly 20% per year, and is responsible for 21% of the growth of GDP in mature economies.

There are alternatives to the Internet. People can mail a letter. They can travel to meet a customer. They can walk into a shop to buy books. They can smudge their fingers as they read a newspaper. However, not using the Internet is rapidly becoming equivalent to not participating in society. The loss of efficiency and the loss of aggregate benefits of participating in a global telecommunication network is a very high cost.

People pay for privacy all the time. They put up curtains. They tint their car windows. There are several companies that promise private email: and people pay for that. Now that people know that every email, every Internet transaction and every interaction is being intercepted, some will pay for privacy by avoiding email, shopping in person, or going to the library to do research. Since much of the benefit of the Internet depends on “network effects,” if even a small percentage of people stop using the Internet, the impact to network value and efficiency is significant. An Australia in which everyone is spied upon when they use the Internet is a less collaborative, less productive, less rich Australia. Ditto the world.

Request for Reform – Stop Mass Surveillance, and Provide More Oversight

The transformative gifts of the global Internet are incredibly fragile and now under very real existential threat. As technologists, it is unconscionable to us that the actions of some governments threaten to destroy one of the most democratic, egalitarian and beneficial technologies in history.

The trust that has been destroyed by surveillance overreach will take a long time to regain. This will require sustained global efforts across politics, law, and technology. Parliament must be willing to rein-in mass surveillance, defend privacy rights and remove the threat to efficiency, productivity and innovation posed by a faulty TIA Act.