Submission No 198

Inquiry into potential reforms of National Security Legislation

Organisation: Australian Interactive Media Industry Association, Digital Policy Group

EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS

Inquiry into potential reforms of
National Security Legislation by the
Joint Parliamentary Committee on Intelligence and Security

Submission

7 September 2012

The Australian Interactive Media Industry Association's Digital Policy Group (**DPG**), which counts eBay, Facebook, Google and Yahoo!, among its founding members, welcomes the opportunity to make this submission to the Committee to assist in its consideration of the proposals outlined in the *Equipping Australia Against Emerging and Evolving Threats* (**"Discussion Paper"**).

DPG is committed to ensuring that Australia is well placed to enjoy the benefits that the internet and online services can deliver to the Australian economy and society. A recent study estimated that the direct contribution of the internet to the Australian economy was worth approximately $50 billion, equivalent to 3.6 per cent of GDP in 2010[1]. That is expected to increase by at least $20 billion over the next five years to $70 billion. DPG's members deliver services that are enjoyed by millions of Australians every day. We also provide platforms that support Australian innovators and entreprenuers, who are able to build and improve their own businesses utilizing the services we offer.

The digital industry is also committed to ensuring that people have a positive experience online. To achieve this, it is vital that we retain the confidence and trust of our users and maintain the security of their data. All DPG members, consequently, have policies that prohibit the use of their services for illegal activity. Unfortunately, just as there are offline, there are occasions when people misuse our services and jeopardise the safe experience our users. Our common goal is to respect the balance between law enforcement's need for information and the privacy rights of the people who use our site. Each DPG member realises this goal through rigorous policies and procedures. Their respective approaches are outlined in more detail in Appendix A.

The Discussion Paper touches on a wide range of issues relating to national security matters, telecommunications sector security and interception reform, as well as Australian intelligence community legislation reform. As the Committee conducts its inquiry and develops recommendations to the Australian Government, the DPG encourages it to have regard to the following principles in shaping any legislative reform with respect to:

(i) how law enforcement obtain lawful access to user data held by service providers; and

(ii) what data retention obligations, if any, could be reasonably imposed on service providers.

We believe that law enforcement should have effective methods to address crime that are proportional to the impact on citizens and companies. We believe that narrow, targeted, proportional rules should always be preferred over blanket rules requiring massive data retention and accessibility. Blanket rules requiring data retention and accessibility are blunt tools which have the potential to infringe on civil liberties and constrain economic growth.

In our view, the Committee should shape any recommendations with respect to lawful access and data retention obligations against the following principles

[1] The Connected Continent: How the internet is transforming the Australian economy, Deloitte Access Economics, August 2011 https://www.deloitteaccesseconomics.com.au/uploads/File/DAE_Google%20Report_FINAL_V3.pdf, page 2

Lawful Access Principles

1. Proportionality: Users enjoy privacy rights and have a legitimate expectation of privacy for the data they share online. Accordingly, provisions that empower law enforcement to obtain lawful access to user data held by service providers must be limited in both time and scope to focus on particularised information relevant to a criminal investigation.

2. Due Process: Service providers should be required to disclose account content and communications only by a search warrant or other court or tribunal process that has been issued based on meeting the standard of probable cause as assessed by a judge or equivalent public official.

Further, targeted and proportionate investigation of criminal offenses is available to Australian law enforcement through appropriately authorised judicial warrants or international standards like the Mutual Legal Assistance Treaties (MLAT) that the Australian Government has entered in to with various different foreign governments. This international standardised process allows a court or judge to ensure proportionality of each request is tested before data is accessed.

3 Efficiency and Cost: Laws granting lawful access should impose the costs of fulfilling those requests on the law enforcement authorities that request the information, and not directly or indirectly on service users. Financial constraints can serve to place an institutional check on the over-use of orders.

4. Transparency: Law enforcement agencies should publicly provide citizens with the full information they need to exercise their democratic right to hold agencies accountable for when and why they issue demands to online service providers for user information.

5. Jurisdiction: Domestic legislation should account for existing legal obligations on providers that arise from the jurisdictions where data is stored and controlled and avoid imposing mutually exclusive or conflicting requirements.

This principle of jurisdiction is informed by the fact that online companies offer services accessed via the Internet across the globe. Consequently, we face the real prospect of many different governments identifying new national legislation on lawful access as the means to achieve security objectives in respect of services like ours.

We are concerned about the potential for chaotic situation of conflicting legal requirements and overlapping jurisdictions for and against disclosure in different countries (countries where the data are stored, or where the law enforcement authorities are based, where the users of the service are located or where the personal data are controlled, etc.). Were this situation allowed to develop, it must be likely that law enforcement will be impaired rather than enhanced in Australia and across the globe.

We therefore believe that it makes more sense to sustain and where necessary reform existing models of cooperation within uncontested jurisdictional boundaries.

Data Retention and Preservation Principles

1. Proportionality: We do not support mandatory data retention requirements which would introduce an obligation to generate data not required for business purposes and to retain it specifically and only for law enforcement purposes. Such a move would be a significant change in policy and one which would have a considerable commercial impact, an impact on public confidence and would create significant administrative challenges for global communications providers.

Mandatory data retention requirements would generally require companies to keep excessive data about their users for longer than is necessary. There are less intrusive and more proportionate and effective policy options that are readily available to Government, such as the power to request preservation of identified data for individual targets and reforming the MLAT process for cross border requests.

MLAT is a government-to-government process controlled by Treaty. The respective governments control the speed with which MLATs are handled. Therefore the efficacy of the MLAT process is fully within the power of government and is contingent on willingness to devote additional resources to speed up that process. It is misplaced to seek to pass legislation to impose new and onerous obligations on industry for perceived shortfalls in government controlled processes.

2. Due Process: Mandatory data retention rules open an assumption of guilt across the entire population. A system allowing for requests for preservation and retention of user data made by a judge or authorised law enforcement officials would lessen the risk from such blanket intrusion into privacy.

3. Transparency: The government should publicly provide citizens with the information they need to exercise their democratic right to hold agencies accountable for when and why they ask companies to store and give them user data.

4 Efficiency and Cost: The costs of fulfilling law enforcement requests should be met by the law enforcement authorities that request the information, and not directly or indirectly on service users.

5. Jurisdiction: Domestic legislation should account for existing legal obligations on providers that arise from the jurisdictions where data is stored and controlled and avoid imposing mutually exclusive or conflicting requirements.

Many online companies offer services globally and therefore potentially face different legislative requirements with respect to data retention laws, if implemented. This has the potential to lead to conflicting legal requirements. Many companies have made commitments to privacy regulator to delete data within a timely fashion, and some have negotiated specific settlements or undertakings to delete data within a certain time period.

We therefore encourage the Committee to sustain existing models of cooperation within uncontested jurisdictional boundaries.

Appendix A

eBay

eBay is Australia's leading online marketplace and has nearly 7 million Australians visiting per month.

eBay partners with Government on cyber security matters. Among the tools that are used to support law enforcement's efforts combating cybercrime in Australia is the Law Enforcement Portal (LEP), a web based tool that allows registered and approved law enforcement officials to obtain eBay user information consistent with eBay's privacy policy.

The LEP tool allows requests to be processed quickly so that law enforcement can proceed with their investigation in a timely manner.

All official requests for information from Law Enforcement and Government offices are recorded in our case management system.

eBay and PayPal have assisted law enforcement agencies in recording nearly 30 convictions based on information provided by LEP in 2010-2011. Convictions have included defendants charged with identity fraud, merchant-related fraud, sales of stolen property, and internal theft.

Our cooperation extends to all levels of law enforcement in Australia.

eBay has provided training to every State and Territory Police force within Australia and also other government agencies such as the Australian Quarantine and Inspection Service (AQIS), Australian Competition and Consumer Commission (ACCC), Australian Crime Commission (ACC) and consumer protection bodies. These trainings cover a wide range of issues, including how eBay's services work, how to obtain records from eBay for an investigation, and changes in investigative techniques in the Internet age.

Facebook

Facebook's mission is to help give people the power to share and to make the world more open and connected. Over 950 million people are using Facebook on a regular basis across the globe, including over 11.5 million people in Australia.

Each month, Facebook enables every one of these users to share information – photos, status updates, and private messages – with their friends. For example, Australian researchers tracking Cockatoo movements have created a Facebook Page to invite people to report, often with photos, sightings of the tagged birds. With over 1,200 people signed up to the Page to receive information about the project, people are able to see their photos and learn about other locations that the cockatoos visit.[2] Another example is the small Australian fashion business MIISHKA has built her business on Facebook, enjoying 300 percent sales growth last year and attracting an

[2] http://theconversation.edu.au/social-media-turns-sydney-residents-into-cockatoo-trackers-5981

88,000-strong fan base.[3] Given the essential role that Facebook plays in the day-to-day engagements of Australians households and businesses, it is vital that we retain the confidence and trust of our users and maintain the security of their data.

Our Statement of Rights and Responsibilities[4] and our Data Use Policy[5] underpin Facebook's relationship with its users.

We undertake numerous activities to ensure users understand these policies and are able to make use of the controls we provide for them. There is a comprehensive online Help Centre[6] and an extensive User Operations function operating 24 hours a day via four locations around the globe.[7]

We respond to requests from law enforcement authorities around the world according to our terms of use and applicable law. We have established processes for law enforcement authorities to submit requests and these are set out in published guidelines.

In order to ensure that our processes are well-understood, Facebook security representatives have provided workshops for Australian police officers who act as Single Points of Contact (or SPOCs) for their force. The Australian law enforcement authorities are therefore very familiar with these voluntary processes and make good use of them. We also publish Law Enforcement Guidelines to provide operational guidelines for law enforcement officers seeking records from Facebook.[8]

We respond expeditiously to Australian law enforcement requests, making sure that we prioritize any cases where there is an imminent risk of death or bodily harm.

In certain cases, a request may only be fulfilled by using the Mutual Legal Assistance Treaty (MLAT) process, which permits the Australian government to make a formal request of the US government to obtain evidence maintained in the United States.

Google's Approach to Security

Every day millions of people trust Google products and services to manage their daily lives and interests. That's why we're so invested in security and constantly at work to stay one step ahead of the bad guys.

Protect user data.

We use a defense-in-depth approach that is multi-layered to help prevent any one system from becoming a single point of failure, including a combination of automated tools and manual review to help keep our services secure and detect any abuser or suspicious activity in our system environment.

---

[3] http://www.dynamicbusiness.com.au/entrepreneur-profile/building-a-sustainable-fashion-business-one-like-at-a-time-27062012.html
[4] https://www.facebook.com/legal/terms

[5] https://www.facebook.com/about/privacy
[6] https://www.facebook.com/help/?ref=pf
[7] More information about our user operations team is provided in this note to the Facebook Safety Page: https://www.facebook.com/fbsafety/posts/331112966969938
[8] https://www.facebook.com/safety/groups/law/guidelines/

Our servers are designed for redundancy and resiliency, such that your data is available to you virtually anytime and anywhere with an Internet connection — even in the event of a disaster.

Protect user activities online.

We design security and resilience into our products from the ground up, as well as the platforms that users use to connect to our services and others. Our automated scanners use data to protect millions of users each day from malware, phishing scams, fraud, and spam.

We think giving you a method to verify your ownership of your account is an important part of improving online security. Two-step verification, our opt-in system for signing in to your Google Account with an extra one-time code on top of your password, significantly reduces the chance of users' accounts becoming compromised via password phishing or guessing.

Contribute to the broader Internet community.

We believe that security is beyond the reach of technology alone, and requires a blend of technology, public policy, and industry engagement. At every turn, we strive to make our technologies available to other developers to improve the overall security of the Internet.

Security is ultimately a shared responsibility, and Google is focused on developing technology to protect users across the web, contributing research, facilitating industry initiatives and conversations, and empowering users through security education.

We take a stand on complex security industry issues and push for open standards and swift action to push the industry forward.

Employ top security talent.

Google has a team of over 250 full-time, world-class security engineers whose job is to maintain the security of user data and Google's infrastructure. Security is a core part of our culture and is baked into our employee training and everything that we do. Hundreds more work on security, abuse, compliance, and related topics through direct association with product and project teams.

Our security engineers range across the company, advising development teams on security features and researching new security innovations to building state of the art intrusion detection systems and responding to reported software vulnerabilities in a timely manner. We work hard on many different aspects of security to better protect information and to push the industry forward.

These engineers are experts in a variety of fields, including developers of popular open source tools, software vulnerability researchers with industry recognition for high-quality findings, and more.

Be open and responsive.

It's a common misconception that open source software is inherently less secure or easier to hack than 'closed' software, but open source projects tend to have fewer vulnerabilities than closed source software. We actively encourage the highly engaged developer community to scrutinise the source code, and offer suggestions about how to tighten up the security infrastructure.

It's a reality that code will always have bugs. We act quickly to respond to and mitigate security threats, and reward those who come to us first so that we can address threats before they are exploited.

Yahoo!7

Yahoo!7 is one of the most comprehensive and engaging online destinations for Australian consumers and advertisers. Formed as a 50-50 partnership between the Seven West Media Group and Yahoo! Inc. Yahoo!7 brings together the successful Australian internet business, Yahoo! Australia & NZ, and the online assets and television and magazine content of the Seven Network, one of Australia's leading media companies. Yahoo!7 has a significant local presence employing over 360 people based across our businesses in Australia and New Zealand.

Safety, transparency and responsiveness are top line priorities for Yahoo!7. We work closely with Australian law enforcement agencies to provide assistance when Yahoo!'s services are being used for criminal activity. This includes the establishment of a 24 x 7 compliance function with a dedicated direct telephone line that can be used for immediate response to emergency law enforcement requests.

Yahoo!7 provides training to the law enforcement community to increase awareness of how Yahoo! products and services work and how to obtain information from us. Yahoo!7 has created an Australian Law Enforcement Process Guide designed to ensure that law enforcement personnel are familiar with Yahoo!7's policies, procedures, and systems, and clearly understand how to obtain the appropriate investigatory information.

Yahoo!7 has a designated Australia-based contact person who deals with all law enforcement requests and ensures cooperation in a timely manner.