Google Australia Pty Ltd
Level 5, 48 Pirrama Road
Pyrmont NSW 2009

Tel: 02 9374-4000
Fax: 02 9374-4001
www.google.com.au

12 May 2014

The Executive Director
Australian Law Reform Commission
GPO Box 3708
Sydney NSW 2001

By email: privacy@alrc.gov.au

SUBMISSION to ALRC Discussion Paper 80

Google is pleased to have this opportunity to provide further input to the ALRC's consideration of privacy in the digital era.

We provide comments on the following matters to inform the ALRC's Discussion Paper process:

- The roles played by government, industry, and individuals in protecting privacy online
- The proposal for a new tort for serious invasions of privacy
- The importance of an effective safe harbour for online intermediaries
- The proposals for new regulatory mechanisms
    - Proposal for a new Australian Privacy Principle for destruction or de-identification of personal information
    - Proposal for regulator to give take down orders for serious invasions of privacy

Kind regards

Ishtar Vij

Ishtar Vij
Public Policy & Government Affairs
Google Australia

EXECUTIVE SUMMARY

Over the past decade, the Internet has caused a major shift in the Australian economy and society, and going forward, its transformative impact could be equivalent to the widespread adoption of electricity.

By bringing consumers and business together, the Internet has ignited an explosion of economic activity – lowering barriers and increasing efficiency for business, and empowering consumers with information and choice. Deloitte Access Economics estimates that the Internet contributes $50 billion directly to the Australian economy and a further $53 billion in non-GDP benefits to households around the country.[1]

With the Internet becoming increasingly important to the economy and participation in society, Australians need to be equipped and empowered as capable digital citizens in order to maximise the benefits. Privacy and security are critical.

There are powerful market dynamics that motivate online service providers to offer strong security and give people the tools they need to proactively manage their privacy. This is crucial to the commercial success of online services as it is fundamental to gaining and maintaining a loyal consumer base.

Google's focus is on keeping people's information safe, secure and always available to them. We work continuously to ensure strong security as the foundation of privacy, to protect people's privacy, and to make Google services more effective and efficient for consumers.

The open nature of the Internet creates much of its value. Intermediaries operate open platforms that underpin innovation and creativity on the Internet, and appropriate limitations protecting them from liability for the actions of others plays a critical role. Before any decision to introduce a new privacy tort is made, it is crucial to carefully consider the implications. Further, it is essential that any new privacy tort does not put intermediaries in the untenable position of policing content or hold them strictly responsible for the activities of users of their services.

Google believes that people should have the ability to access, rectify or delete data that they themselves publish online. For information published by third parties, in line with industry best practice, Google has policies that prevent the use of services to reveal the personal information of others and tools to enable reporting and removal. Given that industry already provides mechanisms to enable people to request deletion, it is not clear that a new regulatory takedown regime is needed.

The overall societal and economic benefits delivered by the Internet must be part of any consideration of privacy online. Attributing an inappropriate weight to the significance of these benefits may act to constrain innovation leading to a negative impact on the entire economy and consumer welfare.

---

[1] Deloitte Access Economics, The Connected Continent, August 2011; www.deloitteaccesseconomics.com.au/uploads/File/DAE_Google%20Report_FINAL_V3.pdf.

1. Protecting privacy online

Google agrees with the ALRC that responsibility for protecting privacy online lies not just with the organisations that collect, store, process or disclose information, but also with individuals.

In order to participate fully in the modern economy, Australians need to be equipped and empowered to be capable digital citizens. Being a capable digital citizen includes not only having the necessary skills be to be smart, safe and responsible online, but also understanding the rights and responsibilities that come with online interactions. Australians will all be better off when everyone uses the best security technologies and techniques.

That is why Google strives to design products that empower our users to proactively protect their own privacy by giving them real and meaningful control. We've invested hundreds of millions of dollars in security to help keep our users' data safe and in developing easy-to-use privacy tools.

Google has more than 400 full-time security experts providing design reviews, consulting, and training across the company, as well as building privacy and security technologies into our products.

Google also works hard to protect people's activities across the web to safeguard their privacy from being compromised by malicious actors. For example, our Safe Browsing technology examines billions of URLs, looking for dangerous websites. Each day we find more than 7,500 unsafe sites and show warnings on up to 6 million Google Search results and on 1 million downloads. Every day more than 1 billion people receive this protection against phishing and malware because of the warnings we show; which are freely available and used by Google Chrome, Apple Safari and Mozilla Firefox.

The Google Privacy Centre (linked from the Google homepage) has information and videos that explain in plain English what data Google stores and how we use it to provide people with services like Gmail, Search and more: www.google.com.au/policies/privacy/. The Privacy Centre also contains information about privacy settings our users can choose when they use our products. Google aims to put people in control of their data.

*See the **Annexure** to this submission for more information on the privacy tools that Google has developed to protect its users' privacy online.*

Google also agrees with the ALRC that non-legislative measures such as education play a critical role in empowering individuals to protect their own privacy online. Education to ensure greater understanding of the many technical tools that are available to Australians to manage their privacy online is of the utmost importance. Google is focused on educating our users about the steps we take to protect them, and the tools that are available to protect themselves on the web.

The Google Safety Centre (www.google.com.au/safetycenter/) provides information for our users on managing privacy and security. It gives actionable, common-sense tips:

- *For everyone – to help manage privacy and security, and prevent cybercrime*
- *For families – to help parents navigate through new technologies, gadgets and services in an ever-changing online world*
- *Safety tools – explore Google's easy-to-use safety tools*

Google partners also with the following charities to provide education and support services for children: The Alannah and Madeline Foundation, Reachout.com by Inspire Foundation, Bravehearts, NAPCAN, Kids Helpline and the Young and Well CRC.

For example, Google supports The Alannah and Madeline Foundation's eSmart Schools program that aims to reduce cyberbullying.[2] The Foundation promotes the positive use of technology and the program is designed to create genuine cultural change within whole school communities when it comes to online safety.

[2] Google and the Alannah and Madeline Foundation team up to improve cybersafety in schools, http://google-au.blogspot.com.au/2013/12/google-and-alannah-and-madeline.html.

2. Proposals 4 to 10 for a new statutory cause of action for serious invasions of privacy

For a cause of action to be introduced, it should be clear that any harm to be addressed outweighs the potential costs arising. For example, one cost is from additional compliance burdens from the implementation of a cause of action.

Should a decision be made to introduce a statutory cause of action for serious invasions of privacy, the cause of action should only be available:

- To natural persons.
- Where a person in the position of the plaintiff would have had a reasonable expectation of privacy in all the circumstances.
- Where the court considers that the invasion of privacy was serious, having regard to whether the invasion was likely to be highly offensive to a person of ordinary sensibilities.
- Where the act complained of was intentional or reckless.
- Where the court is satisfied that the plaintiff's interest in privacy outweighs the defendant's interest in freedom of expression and any other broader public interest.

As outlined in our submission in response to the ALRC's Issues Paper, no action for breach of privacy should be available where a person has previously consented to the conduct that they have complained of. While Google notes that the ALRC has declined to recommend a defence of consent, we welcome the ALRC's recognition that in determining whether a person had a reasonable expectation of privacy in the particular circumstances, a court should have regard to whether or not the plaintiff had consented to the conduct that is said to compromise their privacy.

3. Proposal 10–7 for a safe harbour scheme to protect Internet intermediaries from liability for serious invasions of privacy committed by third party users

As an open platform, the value that the Internet creates is underpinned by intermediaries, which, at scale, facilitate exchanges between people. Appropriate limitations protecting intermediaries from liability for the actions of others have, and continue to play, a critical role in the Internet's development by allowing intermediaries to drive growth, innovation, and creativity.

Google welcomes the ALRC's recommendation that if a privacy tort is enacted, Internet intermediaries should have the benefit of a safe harbour to protect them from liability for invasions of privacy committed by third party users of their service. It is essential that any new privacy tort not put intermediaries in the untenable position of policing content or hold them strictly liable for the activities of users of their services. As the ALRC notes, Internet intermediaries are not in a position to identify content that invades a person's privacy, until it is authoritatively brought to their attention.

The ALRC seeks comment on what conditions should be imposed on Internet intermediaries in order for them to be able to rely on a safe harbour defence. Google submits that a safe harbour should have at least the following features:

- **Definition**—there should be a broad and flexible definition of services that qualify for safe harbour protection. Given that technological change can render legal language obsolete, safe harbours should not be limited to an enumerated list of services or technologies.

- **Notice**—the steps that an intermediary is required to take upon receipt of a valid notice should be clearly set out. This should include providing notice, to the extent reasonable, to a user that a privacy claim has been made with respect to content uploaded by them, and allowing that user an opportunity to provide any relevant information such as a counter notice.

- **Form of notice**—consideration could be given to whether a ruling from an independent party, such as a court, should be required in order to trigger a response obligation. At a minimum, a safe harbour should clearly define the standard of notice or knowledge that triggers a response obligation. Intermediaries should not be expected to arbitrate as to whether a serious invasion of an individual's privacy has occurred.

- **Monitoring**—there should be no requirement on intermediaries to monitor for privacy violations. Any obligations to monitor or proactively look for potentially unlawful content would undermine the purpose of the safe harbour regime.

- **Underlying dispute**—consideration should be given as to whether there should be a requirement for the person making a privacy complaint to first seek removal from the person who has made the content available. The person responsible for the content, and the person most capable of making it inaccessible online, is the person who put it up in the first place. Accordingly, anyone asking an intermediary to remove third party content should document or attest that they have tried and failed to solve the problem at its source.

4. Proposed new regulatory mechanisms

4.1. Proposal 15–2 for a new Australian Privacy Principle for individuals to request destruction or de-identification of personal information that was provided by them

It is industry best practice to provide people with the means to access, rectify, delete or remove data that they themselves intentionally publish online. As discussed above, Google provides people with the tools and mechanisms to do this. We support the following broad principles:

- A consumer should have full control over, including the ability to delete, data he or she publishes intentionally.
- Online hosting platforms should give a user the ability to delete information he or she uploads as well as the ability to delete his or her account.
- Deletion initiated by a user should be carried out in a timely manner by the hosting platform, although some delay should be allowed to prevent, for example, the abusive deletion of content if an account is compromised.

Google provides users with the tools to do this for the data they choose to give to Google.

A Google user can easily access 'account settings' and either:

1. *Delete all information associated with their Google Account entirely.*
2. *Download data that they have created or imported into a number of Google products so that they may close their Google Account and use another provider of their choice.*[3]

The Google Takeout tool allows users to customise a data archive to download a copy of data from Google products. Google Takeout is currently supported for 16 products and counting, including Gmail, Drive, Calendar, YouTube, Google+ and Contacts. See www.google.com/settings/takeout.

The ALRC notes that its proposal does not cover an individual requesting the deletion of information that is published by other individuals or organisations. This is an important limitation.

Some further limitations to consider are:

- Sharing by individuals—where material published online is copied and re-published elsewhere by other individuals, the original hosting platform should not be expected to expected to maintain control over other copies of the material.

[3] Google, 'Download your data: FAQ', https://support.google.com/accounts/answer/3024190.
[3]

- Security—hosting platforms should not be obliged to delete materials when doing so would be likely to undermine the security of the service or allow for fraud.
- Collaborative works—hosting platforms cannot be expected to delete materials created collaboratively at the unilateral request of a single contributor. In cases where clear ownership of a collaborative document is not clear – as in the case of wikis or usenet posts – the questions are more complex.

4.2 Question 15–2 regarding whether to recommend regulator take down orders to remove information that is a serious breach of privacy, whether provided by that individual or a third party

Google submits that there is no demonstrated need for a legislated take down scheme to give effect to this, as the market has already developed innovative and responsive mechanisms. Further, if a new cause of action for serious invasions of privacy were to be introduced, third party content could be addressed through this avenue. As a judicial avenue, there would be significant oversight with regards to the balancing of freedom of expression and other public interests.

As discussed above, Google believes that people should have the ability to access, rectify, delete or remove data that they themselves publish online. Self-help mechanisms are able to operate much more swiftly than any regulatory mechanism would be able to.

Google submits that a regulatory takedown regime for information that has been provided by third parties is not necessary as the market has already developed innovative and responsive mechanisms.

Google has policies and guidelines in place that set out acceptable content and conduct. For example, the YouTube Community Guidelines[4] prohibit use of YouTube for *harassment, invading privacy, or the revealing of other members' personal information*. Users are warned that postings that breach these policies and guidelines will be removed, and that they may be permanently banned from using the site.

Google provides simple and effective ways for users to register complaints about content that breaches these guidelines. Industry leading tools such as the YouTube flag system[5] enable users to report content that they believe has breached their privacy. We respond quickly to these complaints: we have processes for reviewing complaints from users and other parties – 24 hours a day, seven days a week, and we rapidly remove content that is found to be in breach of site guidelines.

[4] https://www.youtube.com/t/community_guidelines.
[5] https://support.google.com/youtube/answer/2802027?hl=en.

Annexure

Tools that Google has developed to protect its users' privacy and security

- **Session-wide SSL encryption** is the default when users are signed into Gmail, Google Search, Google Docs and many other services. This protection stops others from snooping on our users' activity while they are on an open network, such as when a user is accessing the Internet at a coffee shop. Even when users are not signed in to a Google Account, they can avail themselves of session-wide SSL encryption by simply adding an "s" after the http:// in "http//google.com."

- **2-step verification** provides a stronger layer of sign-in security by requiring a verification code in addition to the password.[6] Even if a user's password gets stolen, the thief will not be able to access that user's account. We offer this protection, for free, to any account holder.

- **Safe Browsing** a service that currently flags up to 7,500 sites a day for phishing malware and reaches about 1 billion users across the web. We make our Safe Browsing API freely available to other browsers and services, many of which utilize this service.

- **Google Dashboard** allows our users to change the settings for many Google products from one central location.[7] Within Dashboard, users can exercise control over information that is collected by Google for example by:

    - **Reviewing Web History** and granularly removing items from searches that are conducted while signed in to a Google Account. Within the Web History settings users can pause their Web History, meaning future searches are not stored.

    - **Managing Gmail chat settings** to choose not to store chat history.

    - **Managing privacy settings in YouTube** by choosing to keep likes private, as well as deciding who can send them messages and share videos with them.

- **Google's Ads Settings page** enables users to add or edit information to affect what kinds of ads Google displays. Users also can block specific advertisers from showing ads on Gmail or Google Search, or opt out of seeing customized ads altogether.

- **Google+** puts our users in control over what information is shared and who can see it. With Circles, it is easy to share relevant content, like Google+ posts, YouTube videos, or Local listings, with the right people at any time our users choose.

- **Google Takeout** allows users to customise and download an archive of data stored in Google products.

---

[6] Google, 2 Step Verification, http://www.google.com/landing/2step/?utm_campaign=en&utm_source=en-ha-na-us-sk&utm_medium=ha.
[7] Google, Dashboard, www.google.com/dashboard and www.youtube.com/watch?v=ZPaJPxhPq_g.