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

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

25 November 2013

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

By email: privacy@alrc.gov.au

Dear Sir/Madam

ALRC Issues Paper 43

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

Google believes that there are huge benefits for society being generated in the online environment. This is demonstrated by the explosive growth in use of the Internet in the last decade. It has also been acknowledged by the OECD Council. In a recently released Explanatory Memorandum setting out the background to its recommendations for updating the OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, the Council noted:

> *Over the last three decades, personal data have come to play an increasingly important role in our economies, societies and everyday lives. Innovations, particularly in information and communication technologies, have impacted business operation, government administration, and the personal activities of individuals. New technologies and responsible data uses are yielding great societal and economic benefits.*[1]

Online tools and services have delivered great benefits to the way people conduct their lives, including the way we bank, pay bills, find partners, friends and restaurants, buy and sell goods including art, real estate, books and groceries and educate, study and conduct research. Deloitte Access Economics has put a value of $53bn on the benefits to households.[2]

---

[1] OECD, 'Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/2013-09-09_oecd-privacy-guidelines_EN.pdf.

[2] Deloitte Access Economics, The Connected Continent, August 2011, http://www.deloitte.com/assets/Dcom-Australia/Local%20Assets/Documents/Services/Corporate%20Finance/Access%20Economics/Deloitte_The_Connected_Continent_Aug_2011.pdf.

These overall societal and economic benefits must be part of any consideration of privacy online. It is for this reason that even in the first OECD Guidelines, there was already emphasis on dual policy objectives of privacy protection and enhancement of cross-border data flows. Policy makers must seek to ensure that policies and laws on data collection and use are not unduly restrictive. Failure to do this may constrain data-driven innovation, negatively impacting the entire economy.

Having said that, Google recognises that, as in the offline world, in the online world there is a fundamental need to protect the security and privacy of information. Keeping information safe, secure and always available when our users want it are among our highest priorities at Google. We work continuously to ensure strong security, protect users' privacy and make Google more useful and efficient for them.

In this regard, we support the view expressed by the then Office of the Privacy Commissioner:

> *"...the best approach to enhancing privacy online will be multi-faceted, comprising:*
>
> 1. *principles-based legislation (with specific technology issues dealt with under binding codes where desirable and necessary)*
> 2. *end user empowerment through education*
> 3. *privacy enhancing technology design*
> 4. *international cooperation between jurisdictions."* [3]

1. Google and privacy

User trust is critical to Google's business model and we work hard to keep it every single day. Protecting user privacy means keeping user data secure and enabling users to control their experience online. Clear privacy principles and user-friendly privacy tools are at the core of responsible data stewardship. Our Privacy Policy describes the information that we collect from users, how we use that information, and the ways that users can exercise granular control over the collection, use, disclosure, and retention of that information.[4]

Ensuring that our users' information is safe and secure advances important privacy and security objectives. Our users and the broader public understand that these twin concepts are inextricably intertwined. For example in the US identity theft has now topped the list of consumer complaints reported to the Federal Trade Commission for thirteen years in a row.[5] Measures that reduce the likelihood of identity theft and fraud ultimately foster privacy by

---

[3] Office of the Privacy Commissioner submission to the Senate Standing Committee on Environment, Communication and the Arts review: The adequacy of protections for the privacy of Australians online, August 2010, www.oaic.gov.au/images/documents/migrated/2010-09-06051859/Submission%20Online%20Privacy%20Inquiry.pdf.

[4] Google, Privacy Policy, http://www.google.com/policies/privacy/.

[5] FTC, 'Top 10 Complaint Categories for 2012', http://ftc.gov/opa/2013/02/sentineltop.shtm.

ensuring that data is used and maintained in a way that comports with our users' expectations. That is why we've focused on educating our users about the steps we take to protect them and the tools available for users to protect themselves across the web.

For example, Google's Good to Know (www.google.com/goodtoknow) site provides actionable, common-sense tips for users to help reduce the likelihood of identity theft and fraud. The site offers general advice for users to protect themselves from identity theft and fraud, as well as specific information about how Google helps prevent identity theft and fraud within our products and services.[6]

We also provide our users with built-in-security protections and additional security tools to help ensure that their data is protected. These tools include:

- **Session-wide SSL encryption**, which is the default when you're 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**, which provides a stronger layer of sign-in security by requiring a verification code in addition to the password.[7] 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 10,000 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 to protect their users.

We work continuously to protect our users' privacy. We've invested hundreds of millions of dollars to develop easy-to-use privacy tools and to help keep our users safe online. When it comes to the information shared with Google, we give our users control. For example:

- **Google Dashboard** allows our users to change the settings for many Google products from one central location.[8] Within Dashboard, users can exercise control over information that is collected by Google for example by:

[6] See Google, Good to Know, http://www.google.com/goodtoknow/online-safety/identity-theft/ and http://www.google.com/goodtoknow/protection/identity/.
[7] Google, 2 Step Verification, http://www.google.com/landing/2step/?utm_campaign=en&utm_source=en-ha-na-us-sk&utm_medium=ha.
[8] Google, Dashboard, www.google.com/dashboard and www.youtube.com/watch?v=ZPaJPxhPq_g.

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

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

- **Managing privacy settings in YouTube** by choosing to keep likes and subscriptions 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.

2. Guiding principles for this review

Google is broadly in agreement with the proposed guiding principles set out in the Issues Paper. We would however like to draw attention to the following matters that we consider to be of central importance to the ALRC's review of privacy in the digital era:

- ***The need for flexible, forward-looking and adaptive data policy***

Data policy is the next frontier in technology law. The internet ecosystem - and the economic activity it generates - has delivered and will continue to deliver great societal and economic benefits[9]. But these benefits will only be fully realised if policy makers ensure that data policy is flexible and forward looking, and capable of adapting to the rapid pace of technological change.

Data-driven innovation (ie, the products, services, and processes enabled by data and developed to support smart uses of data) is also vital to Australia's national economic development and its participation in the global digital economy.

The OECD recently highlighted the potential role of data and data analytics to drive innovation and sustainable growth across the global economy and society:

> *Economic and social activities have long relied on data. Today, however, the increased volume, velocity and variety of data used across the economy, and more*

[9] For example, Deloitte Access Economics found that the direct contribution of the internet to the Australian economy was worth approximately $50 billion or 3.6% of Australia's Gross Domestic Product (GDP) in 2010. Deloitte Access Economics, The Connected Continent, August 2011.

importantly their greater social and economic value, signal a shift towards a data-driven socioeconomic model. In this model, data are a core asset that can create a significant competitive advantage and drive innovation, sustainable growth and development.[10]

Rigid and inflexible regulations on data collection, storage, and use risk hampering this evolving area. Google believes that policymakers need to understand the power of data, embrace its utility, and carefully address the challenges it raises without sacrificing the potential it offers. The challenge for policymakers is to strike a reasonable balance between protecting individuals' privacy and enabling innovative technologies, which as part of their operation may leverage data that could include information about individuals.

- ***Policy that promotes responsible collection, handling and stewardship of data while recognising that data is essential to protecting online customers and users***

Data is also essential to protecting online users and customers. Online service providers such as Google use it to detect click fraud, botnets, phishers, malware, and other actors or activities that cause harm to our customers and our users. Privacy policy must strike a reasonable balance between facilitating these important uses of data for the protection of online users, while at the same time promoting responsible and ethical ways to use that data.

Example

The Santy search worm, which first appeared on the Web in 2004, used combinations of search terms on Google to identify and then infect vulnerable web servers. Once infected, the webserver became part of a botnet and repeated the seek-and-infect process, quickly spreading the worm across the Web. Huge traffic spikes alerted engineers to the problem, so queries made by the worms were initially easy to identify. As soon as Google engineers recognized the attack, they began developing a series of tools to identify potential Santy queries and then block access to Google.com or flag them for inspection.

In this case, having access to a good sample of log data meant Google's engineers were able to refine an automated security process, quickly solving a problem without unnecessarily interfering with user experience.[11]

[10] OECD (2013), "Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by "Big Data"", OECD Digital Economy Papers, No. 222, OECD Publishing. http://dx.doi.org/10.1787/5k47zw3fcp43-en.

[11] Jess Hemerly, "Public Policy Considerations for Data-Driven Innovation," Computer, vol. 46, no. 6, pp. 25-31, June 2013, http://www.computer.org/csdl/mags/co/2013/06/mco2013060025-abs.html.

- ***Ensuring that privacy regulation is consistent with best international standards***

Web services are inherently global - they provide services in many countries. Privacy law and regulatory frameworks need to be examined in the context of the global nature of these services. Google submits that a guiding principle of this review should be the importance of ensuring - so far as it is consistent with the principles outlined here and Government policy about the importance of the digital economy - consistency in laws affecting national and transnational data flows.

- ***The importance of education in empowering individuals to protect their privacy online***

The Issues Paper is focused for the most part on what *legal* reforms are appropriate to protect privacy in the digital era. Google believes, however, it would be a missed opportunity for the ALRC not to consider the important role of non-legislative measures such as education in empowering individuals to protect their own privacy online.

The OECD Council recently called upon member countries to "consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures which help to protect privacy." [12]

Google submits that the ALRC provides an important opportunity to consider reform initiatives that will improve digital literacy and raise awareness of privacy. Many new technologies in fact improve privacy – for example, the ability to control access to material placed online. Education to ensure greater understanding of the many technical tools that are available to Australians to manage their privacy online is of utmost importance. Section 1 of this submission outlines the many ways Google educates users about how to manage and protect their privacy when using Google products and services.

- ***Avoiding overlapping regulation and remedies***

As the Issues Paper notes, there already exist a range of legal remedies designed to prevent and redress invasions of privacy. It is most likely that a statutory cause of action for breach of privacy would overlap with at least some of these existing laws, as opposed to merely applying to gaps in existing laws.

In view of the cross-border nature of data in global digital environment, Google submits that reform initiatives should be directed mainly towards ensuring the effectiveness of mechanisms to enable privacy protection across borders. In the event that a statutory cause of action is considered necessary, we believe that it should be tailored in such a way as to avoid any overlap with existing regulation and remedies.

---

[12] OECD, 'Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/2013-09-09_oecd-privacy-guidelines_EN.pdf.

- ***Striking a balance between protection of privacy and other values and interests such as freedom of speech***

The recently released OECD Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data contain a new paragraph 3(b) that recognises the potential conflict between the protection of privacy and other fundamental rights.[13] Similarly, the OECD Communiqué on Principles for Internet Policy Making underlines that "[p]rivacy rules should also consider the fundamental rights of others in society including rights to freedom of speech, freedom of the press, and an open and transparent government".[14]

Google submits that the importance of having regard to freedom of speech is arguably even more important in Australia than it is in OECD member countries (including the US, the UK and Canada) that have the benefit of a constitutionally enshrined protection of freedom of speech.

3. Cause of action for serious invasions of privacy

Google submits that for such a cause of action to be introduced, it should be clear that any harm to be addressed outweighs the potential costs arising, for example through additional compliance burdens from the implementation of a cause of action. This would require careful consultation with stakeholders, as well as a detailed review of the current state of the law (including the common law as well as the various Commonwealth, State and Territory laws referred to on pages 41 to 48 of the Issues Paper) with a view to determining whether gaps exist that need to be addressed by a statutory cause of action or rather whether any perceived shortcoming would be better addressed by updating and/or broadening existing laws to reflect technological advances that have the potential to impact on privacy.

In our submission, if, following the comprehensive reviews suggested under the previous paragraph, a statutory cause of action were to be enacted, it should only be available:

- to natural persons
- in circumstances where the person has a reasonable expectation of privacy
- where the act is sufficient to cause substantial offence to a person of ordinary sensibilities
- where the act complained of was intentional or reckless.

Google also submits that the following safeguards should apply:

[13] Ibid.
[14] OECD, Communique on Principles for Internet Policy-Making, www.oecd.org/internet/innovation/48289796.pdf.

- ***Defence of consent***

The existing consent-based approach to privacy - which is in line with international best practice as reflected in the OECD Guidelines - should be reflected in any statutory cause of action. We discuss the relevance of consent in more detail below in our response to the matters raised at paragraphs 166 to 168 of the Issues Paper.

- ***Intermediaries and Notice and takedown***

The Issues Paper seeks comment as to whether a notice and takedown defence, similar to the "safe harbours" in Division 2AA of the *Copyright Act,* or Schedule 5 Clause 91 of the *Broadcasting Services Act,* should be available in the event that a statutory cause of action is enacted.

The role of web intermediaries should be carefully considered in this context. Such entities should not be expected to arbitrate as to whether a serious invasion of an individual's privacy has occurred. The ALRC should consider whether a ruling from an independent party, such as a court order, should be required to trigger the removal of content by intermediaries.

Google also submits that at a minimum a notice and takedown safe harbour for online service providers would be an essential safeguard in the event that a privacy cause of action is enacted. This is critical and reflects the realities that online service providers and hosts do not have knowledge of what is being posted by users of the services. An important part of any safe harbour scheme must also be a recognition that online service providers should not be required to actively monitor their services for potential infringements of any statutory cause of action[15]. It is also important that a safe harbour should be capable of applying to all online service providers. [16]

- ***Public interest***

A person claiming breach of any new statutory cause of action should be required to satisfy the court that the privacy interest being claimed outweighs any countervailing public interests.

- ***Overlapping remedies***

A person who has received a determination in response to a complaint relating to an invasion of privacy under existing legislation should not be permitted to bring or continue a claim based on any statutory cause of action that may be enacted.

---

[15] This is consistent with the safe harbours in Division 2AA of the *Copyright Act* - see subsection 116AH(2).

[16] In this respect, we note that the safe harbours in Division 2AA of the *Copyright Act* currently do not apply to all online service providers, but rather only those service providers who are Carriage Service Providers within the meaning of the *Telecommunications Act 1997*.

- ***Due diligence***

Finally, Google submits that it should be a defence to any new statutory cause of action that the defendant can show that it has exercised due diligence in implementing security and privacy controls that are appropriate for the context of data processing in the relevant circumstances.

4. Other matters raised by ALRC

In what follows in this section we comment briefly on some of the other matters raised by the ALRC in the Issues Paper.

Reviewing the consent-based model of data protection

Like other responsible internet companies, Google provides consumers with adequate disclosure about what information it has collected and how that information may be used. The Google Privacy Centre (linked to from the Google homepage) has information and videos that explain in plain English what data Google stores and how we use it to provide our users with services like Gmail, Search and more. 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.

It should also be kept in mind that individuals have many choices in the online world. They can easily move to a different tool or service if they consider their personal information or security at risk or compromised, or if they have any concerns about the degree of transparency regarding how their personal information will be used.

Recent research by the ACMA also suggests that consumers are actively taking steps to protect their personal data in ways that include providing false, misleading or minimal identity information if they consider that personal information requested does not appear to be needed for the service offered.[17] For example, the ACMA found that 61 per cent of respondents say they would withhold information if it appeared not to be needed for the service offered. It said that:

> *Australians want to keep any transactional identity, such as an online shopping account, within the narrowest parameters possible. They do this, for example, by withholding all information except what is necessary for a successful result.*

[17] ACMA, Sharing digital identity, 2013, www.acma.gov.au/~/media/Regulatory%20Frameworks/pdf/Sharing%20digital%20identity_Short%20report%202%20pdf.pdf.

Discussing this research, ACMA Chairman Chris Chapman said recently:

> *This research suggests Australians balance the rewards and risks of engaging in the online world and are putting some considerable thought into the construction of their digital identities. With personal data becoming a key asset in the digital economy, protecting against unwanted intrusions, embarrassment and financial loss is crucial to how individuals successfully manage their online interactions.* [18]

Data tracking

The ALRC seeks comment on the regulation of online and offline data tracking.

The web ecosystem depends on advertising to make a wide variety of products and services available to web users at no cost. Generally, services that are free are supported through advertising revenue. Without that revenue, users would not have a choice of so many high quality services free of charge.

As the ALRC notes, online tracking systems can be used to provide outcomes that many people desire, such as interest-based advertising (IBA). IBA is generally about trying to make advertising more useful for internet users and advertisers.

The ALRC also notes that many people want to be in a position to control whether or not they are subject to tracking. Google fully supports the right of users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether. For example:

- Google's interest-based ads contain a notice in the actual advertisement indicating that it is a Google ad. The in-ad notice is linked to information about IBA, including our Ads Preferences Manager, which allows users to change the interest categories used to target ads or to opt-out of interest-based advertising altogether.

- With the launch of our Ads Preferences Manager (www.google.com/ads/preferences), Google became the first major industry player to empower users to review and edit the interest categories we use to target ads. The Ads Preferences Manager enables a user to see the interest categories Google associates with the cookie stored on her browser, to add interest categories that are relevant to her, and to delete any interest categories that do not apply or that she does not wish to be associated with.

- The Ads Preferences Manager also permits users to opt out of interest-based ads altogether. Google implements this opt-out preference by setting an opt-out cookie that has the text "OPTOUT" where a unique cookie ID would otherwise be set. We have also developed tools to make our opt-out cookie permanent, even when users

[18] ACMA, Online digital disguises, 2013, www.acma.gov.au/Citizen/Stay-protected/My-online-world/Staying-safe-online/online-digital-disguises.

clear other cookies from their browser (see www.google.com/ads/preferences/plugin). We are encouraged that others are using the open-source code for this plugin, released by Google, to create their own persistent opt-out tools.

As we work to bring more relevant ads to our users, we continually seek to preserve transparency and user control over the information used in our ad system. Our own experience suggests that online users appreciate transparency and control, and become more comfortable with data collection and use when we offer it on their terms and in full view.

Right to removal of certain information

The ALRC has sought comment on whether there should be an enforceable right to removal of certain information online.

Google submits that we need more public debate about the value of such a right and about what should be encompassed in any right to removal of information online. We also need a debate about how any such right should be applied to hosting platforms and search engines.

We think a balanced, reasonable and implementable approach is possible, based on a few principles:

- Firstly, people should have the right to access, rectify, delete or move the data they publish online.

- Secondly, people should not have the automatic right to delete what other people publish about them, since privacy rights cannot be deemed to trump freedom of expression, recognizing that some mechanisms need to be streamlined to resolve these conflicts.

- Thirdly, web intermediaries host or find content, but they don't create or review it, and intermediaries shouldn't be used as tools to censor the web. Search engines serve an important function online, and any right to removal of content that may be enacted should not interfere with their ability to point consumers to information published elsewhere.

Earlier this year, in a case between Google and the Spanish Data Protection Agency,[19] the Advocate General at the EU's Central Court of Justice handed down an opinion that stated that requesting search engine service providers to suppress legitimate and legal information that has entered the public domain would "entail an interference with the freedom of

[19] Google, Judging freedom of expression at Europe's highest court, http://googlepolicyeurope.blogspot.be/2013/02/judging-freedom-of-expression-at.html.

expression" and "amount to censorship".[20] He argued that publishers - not search engines - are responsible for the information they put online. Search engines have no control over the information posted by others. They just point to it.

Google submits that where information is demonstrably legal, and continues to be publicly available on the web, it should not be censored as a result of any right to removal of content that may be enacted. People should not be prevented from learning that a politician was convicted of taking a bribe, or that a doctor was convicted of malpractice. The Internet has allowed unprecedented access to information. In order to achieve all the social, cultural and economic benefits of the Internet, it must be kept free and open.

We think it is also instructive to consider recent research that suggests that users, including young adults, are already actively involved in managing their online reputation in social media. For example, a recent study by Pew Internet found that:[21]

> *'Young adults, far from being indifferent about their digital footprints, are the most active online reputation managers in several dimensions. For example, more than two-thirds (71%) of social networking users ages 18-29 have changed the privacy settings on their profile to limit what they share with others online.'*

Google would be pleased to meet with the ALRC to discuss any of the issues raised in this submission.

Kind regards

Iarla Flynn
Head of Public Policy and Government Affairs
Google Australia and New Zealand

[20] Court of Justice of the European Union, Advocate General's Opinion in Case C-131/12, 2013, http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-06/cp130077en.pdf.
[21] Pew Internet, Reputation Management and Social Media, www.pewinternet.org/Reports/2010/Reputation-Management.aspx.