facebook

23 December, 2013

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

By email: privacy@alrc.gov.au

Dear Professor MacDonald,

Facebook welcomes the opportunity to make this submission to the Australian Law Reform Commission's inquiry – *Serious Invasions of Privacy In the Digital Age*.

At Facebook, we have a strong commitment to privacy and to empowering people to connect and share with the audience that they want. We hope that insights from our experience may be helpful to the Commission as it advances its work.

Facebook is a global communications platform that is embraced by over 12 million Australians. In Australia and internationally, people find a value in connecting and sharing with the people, places and things that matter to them each day via social networks.

Facebook is rapidly becoming an everyday part of life for the majority of online Australians. For example, one Brisbane mother established a Facebook Page to allow parents of multiple births to share stories and find support. More than 530 Australians are members of the Page and have formed friendships via it. Melissa Kirkwood, the Brisbane mother who started it all, was nominated for a Community Spirit medal in the Pride of Australia Awards.[1]

The social web is an engine for jobs, innovation, and economic growth. Facebook is a platform that supports Australian innovators and entrepreneurs in building and expanding their businesses to attract more customers and increase revenues. The McKinsey Report *The Social Economy: Unlocking value and productivity through social technologies*[2] found that social technologies could increase the productivity of interaction workers by 20 to 25% and deliver efficiencies in business processes so that $900 million to $1.3 trillion of annual value could be unlocked by social technologies.

Australian businesses and entrepreneurs are leveraging Facebook for their benefit. For example, the fashion entrepreneur MIISKA built a sustainable business entirely on Facebook, attracting 1,000 unique buyers in the first 6 months and enjoying 100% of revenue being driven exclusively from Facebook.[3] And Half Brick, a Brisbane-based game developer whose game was listed as one of the

[1] www.couriermail.com.au/news/features/twins-advice-page-a-lifeline-for-mums/story-e6freowo-1226416116862
[2] http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy
[3] https://www.facebook.com/miishkafanpage

Top 25 most popular games on Facebook in 2012,[4] is enjoyed by over 2 million people around the world each month.[5]

Before responding to some of the specific questions asked in the Issues Paper, it may be useful context for our specific comments to provide some background about Facebook's policies, tools and outreach on privacy.

Facebook's Strong Commitment to Privacy

Facebook gives people the power to share and connect, in the ways that they want, with the audiences that they want. As Facebook's founder and CEO Mark Zuckerberg has explained, Facebook was created "on the idea that people want to share and connect with people in their lives, but to do this everyone needs complete control over who they share with at all times."[6]

Indeed, trust is the foundation of the social web and people will go elsewhere if they lose confidence in our services. We have adopted industry-leading security practices and protect people's privacy by giving them control over the information they share and the connections they make through our service.

Our commitment to privacy was verified as part of a recent audit conducted by the Irish Data Protection Commissioner (DPC) of Facebook Ireland, the company with whom Facebook users in Australia contract when agreeing to the terms of use on the site. The DPC "found a positive approach and commitment on the part of [Facebook Ireland Ltd] to respect the privacy rights of its users".[7]

In our own efforts to build policies that protect privacy while making the world more open and connected, one lesson that we have learned is that extraordinary care is required to empower individuals to control their own information without creating unintended adverse consequences in other areas, such as freedom of expression. In the legislative context, we encourage the Commission to consider these issues and to make recommendations that will ensure that Australian privacy law is balanced and protects individual privacy, whilst also enabling business certainty and innovation to facilitate the social web. Overly restrictive regulations will prevent online platforms from functioning in the way that individuals expect and desire and the way that Australian businesses need them to, in order to enjoy the economic benefits that sites such as Facebook can deliver.

The Commission should also take into account that protecting privacy requires action by individuals, industry and government. Law alone is unlikely to be a complete solution to protecting privacy and

---

[4] http://newsroom.fb.com/News/545/Top-Rated-Social-Games-of-2012

[5] http://www.theaustralian.com.au/news/jetpack-joyride-in-facebooks-top-25-games-for-2012/story-e6frg6n6-1226531480564

[6] Mark Zuckerberg, "Our Commitment to the Facebook Community" November 30, 2011 https://blog.facebook.com/blog.php?post=10150378701937131

[7] *Irish Data Protection Commissioner*, Report of Audit – Facebook Ireland, 21 December 2011, page 3 (http://dataprotection.ie/viewdoc.asp?DocID=1182).

when making policy recommendations, the Commission should have regard to the fact that industry has a strong incentive to self-regulate and empower individuals to manage their information in an informed way.

Statutory Cause of Action for Serious Invasion of Privacy

The Commission asked what guiding principles would best inform the ALRC's approach to the inquiry, and the design of a statutory cause of action for serious invasion of privacy. The Commission has already outlined the principles it intends to use to inform the development of its proposals for reform, one of which is "the capacity of individuals to engage in digital communications and electronic financial and commercial transactions." We encourage the Commission to consider broadening this principle to recognize the self-expression and innovation that the social web enables. Taking on board these considerations, this principle could be revised, for example, to recognise: "the capacity of individuals to engage in digital communications, electronic financial and commercial transactions, and the self-expression and innovation that the internet enables."

In addition, in crafting a cause of action for serious invasion of privacy, due care must be taken to ensure the integrity of existing law governing privacy. Particularly, in the case of alleged privacy violations by service providers and other companies that handle consumer data, the *Privacy Act* (as amended by the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, whose reforms are scheduled to go into effect this coming March) provides a comprehensive regulatory scheme, including an exhaustive enforcement scheme. Any cause of action for serious invasion of privacy should not extend to cases already cognizable under the *Privacy Act*. A failure to ensure this separation will undermine the integrity of both *Privacy Act* enforcement and the new cause of action, because the overlap will inevitably lead to inconsistent or unclear rules and forum shopping based on those inconsistencies. Maintaining separation between the cases cognizable under each regime will ensure that a cohesive body of case law can develop to provide guidance and predictability to all affected entities. Consequently, we suggest that the Commission may wish to add a new principle to inform its work, namely, "existing, and recently updated, national privacy protections".

Free Expression and Economic Development Consequences Intermediary Liability

The Discussion Paper seeks comment on whether any cause of action should contain a fault element or be based on strict liability. We do not believe any cause of action should be based on strict liability. This is because a strict liability element would create a new and onerous obligation that would be inconsistent with the balance between privacy and the other matters that the ALRC has identified as important. Such an approach may see the privacy cause of action being used as a catch-all to capture causes of action that are already recognizable before the courts (for example defamation, breach of confidence, and trespass). This would be inconsistent with the goals of balancing the need to protect serious invasions of privacy with the ordinary rights and norms associated with freedom of communication and expression, which are otherwise excluded from the causes of action by either the requirement of a fault element, or by statutory or common law defenses.

This is especially true with regard to intermediaries and Internet hosts of user-generated content, which provide the platforms on which people and businesses can communicate. As many policymakers both in Australia and around the world have recognized, imposing liability on a platform for the actions and communications of those who use it disserves the public interest because the threat of liability discourages the availability of open platforms for communication and encourages those who do offer these platforms to do so restrictively. This is true regardless of whether the intermediary is a telephone company, an email service provider, or a social network.

In all of these cases, the intermediaries generally have a limited role in generating or providing the communications that are distributed through their systems and an equally limited ability to know or investigate facts surrounding those communications. In these cases, imposing liability on the intermediary simply makes it more risky and costly to provide an open communications service.

Of course, the general policy of holding people – not their service providers – responsible for their own actions does not mean that intermediaries should be able to evade liability if they are themselves engaging in conduct that is actionable. In cases where an intermediary provides or solicits content that inherently violates privacy, then that intermediary may be subject to liability because it is no longer acting as an intermediary, but instead as a provider of the content. In contrast, where the intermediary merely provides a blank space that users can fill up, the fact that in an individual case a user filled the space with invasive content cannot turn the intermediary into a co-violator. Creating an intermediary platform immunity scheme will provide for business certainty and allow the significant innovations that online platforms enable to continue to thrive.

Cause of action for harassment

The Discussion Paper asks whether, if a stand-alone statutory cause of action for serious invasion of privacy is not enacted, existing law should be supplemented by legislation providing for a cause of action for cyber-harassment. Serious incidents of online harassment are already recognizable under Australian law (for example action may be taken to restrain apprehended violence, or through tort where the conduct amounts to an assault), however, there is no recognized cause of action for harassment generally. It would be incongruous to create a cause of action creating liability for online conduct that would not be the subject of similar liability if the conduct was committed offline.

Facebook shares the Commission's concern that it is important to ensure that Australians have a safe and positive experience online. Before finalizing recommendations on whether a specific cause of action for cyber-harassment is warranted, however, we suggest that it may be useful to take in to account: firstly, the existing laws and proposed government policies relating to online safety; and, secondly, the strong focus of industry on the safety of people online.

Taking each of these in turn-- firstly, existing Australian laws already prohibit the use of carriage services to menace, harass or cause offense.[8] In addition, the new Government undertook, as part of

[8] Section 474.17 of the Criminal Code 1995: http://www.comlaw.gov.au/Details/C2013C00366/Html/Text#_Toc369269838

its election policies to examine existing Commonwealth legislation to determine whether to create a new, simplified cyber-bullying offence.[9]

Secondly, the safety of the people who use Facebook is our top priority. Our Statement of Rights and Responsibilities,[10] which everyone signs up to when they create an account and that are linked to throughout the site, outline what people can and cannot do on our platform. The Community Standards[11] provide a succinct summary of our content policies. Both documents expressly prohibit "bullying and harassment".

Facebook's tools to promote online safety start with our promotion of a real name culture. We believe that people on Facebook are more likely to adhere to community rules and less likely to engage in negative, dangerous, or criminal behavior when their real-world friends and family surround them and they are accountable for their actions.

To protect our real name culture, we've made using a fake name a violation of our policies, and it is grounds for closing an account; we have tools to detect fake accounts; and we block the registration of accounts under we identify as using fake names. Facebook encourages people to report others whose behavior violates our policies.

To assist in enforcement of our policies, Facebook has a robust reporting infrastructure that was examined as part of the audit conducted by the Irish Data Protection Commissioner (DPC) of Facebook Ireland, the company with whom Facebook users in Australia contract when agreeing to the terms of use on the site.

As the Irish DPC explained about our reporting infrastructure:

> *"Facebook provides its users with a variety of ways to report abuses on the site. Users can go to the Help Centre and find pages of information about abuses to report. [Facebook Ireland] also has contextual reporting buttons on every page and associated with every piece of content. On every profile, there is a report link; on every photo there is a report link; and on every advertisement there is a way to report it. There is a means to report abuses included on every profile, photo and advertisement."*[12]

The Irish DPA concluded:

> *"We examined the accessibility of options available to a user who wishes to report an issue to Facebook. It is considered that it is straight-forward for a user to locate the 'Report Abuse' options via the 'help' drop down*

[9] http://lpaweb-static.s3.amazonaws.com/Coalition%202013%20Election%20Policy%20-%20Enhance%20Online%20Safety%20for%20Children.pdf
[10] https://www.facebook.com/legal/terms
[11] https://www.facebook.com/communitystandards
[12] *Irish Data Protection Commissioner*, Report of Audit – Facebook Ireland, 21 December 2011, page 137 (http://dataprotection.ie/viewdoc.asp?DocID=1182).

> *option on the user profile page and within 2 mouse clicks is within the 'Report Abuse or Policy Violations' of the Help Centre'."*[13]

And further:

> *"We are satisfied that [Facebook Ireland Ltd] has appropriate and accessible means in place for users and non-uses to report abuse on the site. We are also satisfied from our examination of the User Operations area that [Facebook Ireland Ltd] is committed to ensuring it meets its obligations in this respect."*[14]

Our reporting infrastructure system leverages the more than one billion people who actively use our site to monitor and report potentially dangerous content. We make it easy to report harmful or harassing content with "report" links on nearly every page on Facebook.[15] People on Facebook regularly use these links.

When people report the content, we are quick to respond. We prioritize the most serious reports and a trained team of global reviewers responds to all reports and escalates them to law enforcement as needed. When someone's actions violate our policies, we can assign corrective action. In serious or potentially criminal matters, this involves account termination or referral to law enforcement.

Right to be Forgotten

As noted above, Facebook was created based on the idea that people want to share and connect with people in their lives but to do this, they must have control of their information. To empower people to exercise this control, we offer tools such as inline privacy controls that allow users to select their audience at the exact time when they are sharing information on Facebook. There are also additional tools that enable people to change the audiences they have selected for their posts, to remove information that they have shared on Facebook, download their information from Facebook, or to deactivate or delete their account.

The Discussion Paper asks whether a requirement should be introduced "that organisations, such as social media providers, permanently delete information at the request of the individual who is the subject of that information." In considering whether a new deletion requirement, it is important to understand that Facebook, like most other social media providers, already enables a right of erasure – namely, that people are able to remove information that they have contributed to a service and that, at that request, that information should be deleted forever. There is no reason to believe that additional legislation is needed to provide people with the ability to erase information they have posted on social media and already have the ability, on Facebook and elsewhere, to delete.

Some interpretations of a right to be forgotten potentially go much further – suggesting that people should have the ability to remove any trace of themselves, including the speech of other individuals, and even if those other individuals chose to keep their speech private. Such an expansive rule has

---

[13] *Id.*, page 141.
[14] *Id.,* page 139.
[15] For an overview of our reporting tools, please see: https://www.facebook.com/report/

appropriately come under significant scrutiny because it substantially interferes with freedom of expression – including the ability to engage in speech that directly promotes the public good, such as news reporting and criticism.

Moreover, such a broad restriction would promote one individual's wishes at the expense of another's privacy, since the other individual will have his or her own right to maintain the integrity of his or her own materials (the so-called "right to remember") and to prevent others from invading private storage that they may choose not to make accessible. For example, if a person kept a paper diary in her home that described her observations about her daily life, giving all of the individuals mentioned in the diary the ability to enter her house and rip out the pages that mentioned them would be fundamentally at odds with the person's own individual rights.

Finally, safety advocates have criticized broad "right to be forgotten" proposals on technical grounds. In today's interconnected world, even if a service provider deletes information, there is no guarantee that a person who received it previously did not make a copy of the information or otherwise distribute it prior to its deletion. This is, of course, no different from the fact that a person receiving a paper letter could make a photocopy of the letter before returning the letter to its sender. In this environment, suggesting – particularly to people who may not fully appreciate these risks – that it is possible to remove all traces of oneself from the Internet may mislead people into making unsound choices about the information that they will decide to share with others.

We suggest that the Commission takes account of the many measures already available to empower Australians to control their information and whether these steps already go some way to addressing the concern that lead to this issue being raised in the Discussion Paper.

Employers accessing social media accounts

The Discussion Paper states that there is a growing concern about the use of social media to assess candidates for work, education and other opportunities. At the time that reports first surfaced that employers or others were seeking to gain inappropriate access to people's Facebook profiles or private information in March 2012, our Chief Privacy Officer Erin Egan, posted a note to our Facebook and Privacy Page, and promoted her message through mainstream media, to reassure the public that they should keep their passwords to themselves and highlighted clause 4(8) of the Statement of Rights and Responsibilities, which prevents the sharing of passwords so that account security can be maintained.[16]

Although it is undoubtedly true that obtaining private account log-in credentials for an employee is a significant privacy intrusion, we believe that the Commission should first analyse whether this issue merits new laws or can adequately be address under the existing, and newly reformed, Australian privacy laws.

[16] https://www.facebook.com/legal/terms

There is a risk that legislative attempts to stop this practice can be overbroad. Given the social web is increasingly a platform through which businesses are improving productivity and driving business growth, there can be work-related social media interactions that do not interfere with an employee's privacy that may be unintentionally caught up in such laws.

****

Please let us know if you would like any additional information on the issues we raise in this submission.

Kind regards,

Mia Garlick
Head of Policy
Facebook Australia and New Zealand