Serious Invasions of Privacy in the Digital Era

Pirate Party Australia

Submission
By Simon Frew
President
Pirate Party Australia

Introduction

Pirate Party Australia would like to thank the Australian Law Reform Commission (ALRC) for the opportunity to submit on the ALRC's proposals regarding serious invasions of privacy.

About Pirate Party Australia

Pirate Party Australia is a political party registered under the *Commonwealth Electoral Act 1918*. The Party was founded in late 2008, and contested its first Federal Election in 2013. The Party's main areas of concern are intellectual property rights reform, privacy rights, increased governmental transparency, and opposition to censorship.

Pirate Party Australia is a member of a worldwide movement that began in Sweden in 2006, and has since spread to more than 40 different countries. Pirate Parties have been elected to all levels government, including 45 state seats in Germany, three seats in the Icelandic Parliament, and two Members of the European Parliament.

General Discussion of ALRC Approach to Serious Invasions of Privacy Proposals

Pirate Party Australia is generally supportive of the proposals contained in the "Serious Invasions of Privacy in the Digital Era" Discussion Paper (DP 80). There are however some proposals that would significantly weaken the efficacy of the proposals as a whole and need to be properly addressed.

The approach sketched out by DP 80 is a vast improvement on the current situation. Pirate Party Australia favours the creation of a new tort to deal with serious invasions of privacy. The proposed definition of a serious invasion of privacy is well structured.

Privacy is an important right that is under threat in our modern society. The ease with which information is shared has created an environment where both corporations and government agencies use the proliferation of the Internet to undermine privacy protections of ordinary citizens. While the proposals in DP 80 go a small way to protecting citizens from serious invasions of privacy, the issue is much larger than addressed here.

An example of this in the corporate realm, is Google's practice of scanning emails to build profiles of customers to target them with advertising.[1] This type of invasion of privacy is increasingly common and many companies track users' browsing habits, scan private messages, mine social media, and so on, to build profiles for marketing purposes.

Governments also engage in invasive monitoring of citizens through warrantless access to telecommunications data (commonly referred to as 'metadata'). This is justified by using an incorrect analogy comparing this to reading the addresses on envelopes. However, metadata gives away much more information about individuals than that. Senator Scott Ludlam correctly explained the issue late last year when he said "Metadata reveals mobile and landline phone records, a person's precise location, the source and destination of electronic mail, their entire social networks [and] web history."[2] There were 293,501 times where law enforcement agencies (LEAs) accessed metadata last year.[3] This is a significant proportion of the population whose data has potentially been sifted through with little justification.

A study into what can be inferred by metadata was conducted by two computer science graduate students at Stanford University.[4] The research was conducted using 546 participants over three months. In an interview with Ars Technica Jonathan Mayer, lead researcher said "We found that phone metadata is unambiguously sensitive, even in a small population and over a short time window. We were able to infer medical conditions, firearm ownership, and more, using solely phone metadata."[5] To demonstrate the private nature of the metadata collected the researchers put forward some of the more sensitive datasets to show just how invasive metadata collection can be. For example:

> Participant E had a long, early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

This is unambiguously private data. Under the current surveillance regime in Australia all of this information can be collected by LEAs without a warrant. Due to the serious invasions of privacy

---

[1] Liam Tung, "Google highlights email scanning practices in terms of service update", *ZDNet* (online), 15 April 2014, http://www.zdnet.com/google-highlights-email-scanning-practices-in-terms-of-service-update-7000028439/

[2] Chris Duckett, "Australia's chief law brands metadata a 'contestable concept'", *ZDNet* (online), 3 December 2013, http://www.zdnet.com/australias-chief-law-officer-brands-metadata-a-contestable-concept-7000023859/

[3] Commonwealth Attorney-General's Department, "Telecommunications (Interception and Access) Act 1979 -- Annual report for the year ending 30 June 2013", available from http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx

[4] Clifton B Parker, "Stanford students show that phone record surveillance can yield vast amounts of information", *Stanford University News* (online), 12 March 2014, http://news.stanford.edu/news/2014/march/nsa-phone-surveillance-031214.html

[5] Cyrus Farivar, "Volunteers in metadata study called gun stores, strip clubs, and more", *ARS Technica* (online), 13 March 2014, http://arstechnica.com/tech-policy/2014/03/volunteers-in-metadata-study-called-gun-stores-strip-clubs-and-more/

metadata enables, Pirate Party Australia believes that access to this information must be more strictly limited and overseen by the judiciary through warrants.

Discussion of Specific Proposals

The proposed approach to balancing competing rights and interests when determining actionability under the public interest test, such as freedom of expression and national security, is a delicate area where striking the right balance is vital for the policy to work effectively. One issue the Pirate Party considers especially important is the line between transparency and privacy in relation to public figures such as politicians. The Pirate Party notes it is especially difficult to decide where the onus should lie in such circumstances.

There are situations where the public interest is obvious and clear, and placing the burden on the plaintiff is a reasonable proposal to prevent litigious individuals from using the threat of Court to chill speech. Pirate Party Australia would like to emphasise the points made in 8.28 and 8.29 of the discussion paper as vital considerations in balancing the competing interests. The bar for bringing an action would be set too high if the plaintiff had to demonstrate that every type of public interest was not outweighing their right to privacy before they could proceed with a case. Equally there are situations where the defendant would be in a position to explain why the private information was released in the public interest that would not be immediately obvious and as such should be recognised as a legitimate defence.

Pirate Party Australia therefore prefers public interest to be a defence, not part of the cause of action.

Proposal 10.1 raises concerns about the potential for abuse by LEAs. Any exception must only protect LEAs from lawful investigations and activities. Should law enforcement officers recklessly or wilfully release the private data of an individual under investigation, the tort should be allowed to proceed. The widespread warrantless access to metadata (discussed above) raises the distinct possibility of abuse, as has been seen in other jurisdictions. There was widespread reporting of US National Security Agency (NSA) agents engaging in a practice called 'LoveInt' where agents would use access to the private data collecting tools to spy on spouses, girlfriends, potential and ex-partners.[6] Considering extremely private data can be accessed without judicial oversight under the current legal regime, there needs to be recourse to address abuse of any access granted should it occur.

Pirate Party Australia supports a safe harbour scheme for Internet intermediaries as outlined in proposal 10.7. The provisions should be broadly defined, however it is reasonable for Internet intermediaries to both provide a method to take down content and enable users to remove content that is found to be a serious invasion of an individual's privacy in order to be eligible for the safe harbour protection.

[6] Edward Moyer, "NSA offers details on 'LOVEINT' (that's spying on lovers, exes)", *CNET* (online), 27 September 2013, http://www.cnet.com/au/news/nsa-offers-details-on-loveint-thats-spying-on-lovers-exes/

Proposal 10.11 gives courts the authority to deliver up or take down offending material. While Pirate Party Australia supports this ability, it must be noted that due to the ease of copying and re-posting there will be many situations where removing content will not put a stop to the invasion of privacy. There are also instances where content will be re-posted on platforms hosted in other countries by people who are not necessarily subject to Australian laws.

The ability of the court to award costs as part of a decision is important to enable more equitable access to justice. The ability to bring an action for a serious invasion of privacy should be available to everyone. Requiring plaintiffs to pay for a lawyer without the ability to recover costs seriously hampers this ability for people on lower incomes.

Pirate Party Australia believes it is highly preferable to have a new tort for serious invasions of privacy introduced. Should the Commonwealth Parliament choose not to enact the new tort, amending the breach of confidence tort to allow compensatory damage for emotional distress is a reasonable approach to better equip the Australian legal system to deal with serious invasions of privacy.

When considering granting injunctions to prevent the publication of private information, as discussed in Proposal 12.2, Pirate Party Australia believes that injunctions should only be granted where the plaintiff has a high likelihood of succeeding in a case should one be brought, taking into account the balance between freedom of expression and privacy as discussed in Section 8. Freedom of expression is a vital aspect of protecting a democratic society. The bar for injunctions should be set high due to the risks they pose to free speech.

Overall the ALRC's approach to the use of surveillance devices is an improvement on the current situation. Pirate Party Australia supports uniform surveillance device and workplace surveillance laws and definitions only if these laws are written to provide adequate privacy protections for Australian citizens. The prevalence and growth of surveillance devices is of concern for a significant section of society and privacy needs must balance against other considerations such as the detection and prevention of crime.

The ability for CCTV cameras, drones and similar tools and devices to monitor what would otherwise be private interactions needs to be adequately limited by privacy laws. In New South Wales there has been pressure applied by the media and NSW Police for local councils to establish widespread networks of CCTV cameras to work around state government restrictions on police use of CCTV to monitor the population.[7]

This type of pressure will continue to increase as technology advances andthe ease of surveillance will grow with it. It is vital for a free and democratic society that protections are carved out to prevent privacy being lost for all.

[7] Robert Carr, "Surveillance politics and local government: A national survey of federal funding for CCTV in Australia", *Security Journal*, 10 March 2014, http://www.palgrave-journals.com/sj/journal/vaop/ncurrent/full/sj201412a.html

The approach proposed in the discussion paper for the privacy implications of ‘wearables’ and ‘drones’ are a reasonable way to deal with the privacy risks posed by the proliferation of these devices. While these technologies offer many benefits, they also represent a threat to privacy in many situations and as such they need to be regulated.

Exceptions for the use of surveillance devices to uncover corruption and other private information that is in the public’s legitimate interest seems to be well balanced. However, such protections should not be limited to professional journalists. The nature of journalism is undergoing a serious transformation. With the decline of traditional media outlets, including the possibility of closure of many regional newspapers,[8] there has been a counterbalancing spread of social media and citizen journalism. If any reference to journalism is needed for the public interest exception to apply, the exception should refer to an ‘act of journalism’ to ensure protection for ordinary citizens engaging in journalistic practices. Otherwise, the public interest exception should simply apply on a case-by-case basis.

[8] Sharri Markson, “Fairfax watchlist: 30 papers may shut”, *The Australian* (online), 12 May 2014, http://www.theaustralian.com.au/media/fairfax-watchlist-30-papers-may-shut/story-e6frg996-1226913732502