Submission to Human Rights Commission: Human Rights and Technology Project

Dr Diarmaid Harkin and Dr Adam Molnar
Deakin University

NOTE: This submission is supported by research funded by the Australian Communications Consumer Action Network (ACCAN).

Human rights and technology

1. What types of technology raise particular human rights concerns? Which human rights are particularly implicated?

The growing commercial availability of 'consumer spyware' poses a number of human rights concerns. 'Consumer spyware' is malware that offers significantly invasive capabilities of surveillance and is sold to general audiences who may wish to place mobile phones, tablets or personal computers under observation. The authors of this submission have been conducting research into the consumer spyware industry (supported by ACCAN) and have examined the software and marketing strategies of a number of companies attempting to sell invasive tools of surveillance to general consumers.

Typical 'spyware' products offer significant powers of surveillance over a target including the ability to remotely collect text messages, photos, videos, recordings of phone/VOIP conversations, real-time GPS location data, internet browsing data, and the capacity to activate the microphone and camera of the target-device for real-time 'eaves-dropping'. Furthermore, a number of spyware vendors provide monitoring of private applications such as WhatsApp, Tinder/Grinder, Facebook messenger, and deploy keylogging functions to reveal the passwords of targets thus permitting access to private email accounts along with professional, banking or social media accounts. Spyware such as 'Flexispy' also offers the ability to send spoof SMS' from the target-device, permitting the 'operator' to impersonate the target without their knowledge. The purchase of such spyware is available on the open-web and using the example of 'MSpy', costs approximately $100 (USD) per month.

The open availability and access to such invasive tools of surveillance poses a number of human rights concerns, particularly with respect to the right to privacy (Article 17). Spyware is a significant threat in a number of contexts. It is most often documented as a threat from states to their citizens and has been associated with a wide-range of human rights abuses perpetrated by governments (McKune and Deibert 2017; Marzcak et al 2015a; Marzcak et al 2015b). Spyware has been deployed maliciously against journalists, activists, and political opponents, and can be a concern in the hands of law enforcement. New South Wales Police for instance spent $2 million purchasing 'FinSpy' with no clarity on whether it was deployed lawfully and in accordance with legal surveillance standards (Farrell 2014). Moreover, spyware is increasingly marketed to general-use audiences with the industry recommending it be used to target children, employees and intimate partners.

2. Noting that particular groups within the Australian community can experience new technology differently, what are the key issues regarding new technologies for these groups of people (such as children and young people; older people; women and girls; LGBTI people; people of culturally and linguistically diverse backgrounds; Aboriginal and Torres Strait Islander peoples)?

The use of spyware has particular implications for women and children. For instance, there is an increasing recognition within the family violence advocacy sector of the threat posed by spyware. In the UK, research by Women's Aid suggested that 29% of abuse victims experienced the "use of spyware or GPS locators" (Women's Aid 2018), the National Stalking Helpline (UK) received 130 reported cases of spyware in 2017 (Lyons 2018), and in Australia, surveys of domestic violence practitioners report that 74% had seen "tracking via smartphone apps" amongst their clients (Re:Charge 2015: 6). Similarly, the National Network to End Domestic Violence (NNEDV) in the U.S has also stated that 72% of victim service providers had clients who were "stalked through the use of a stalking app or GPS or location tracking device" (Southworth 2014: 3). It is clear therefore that the rise of the consumer

spyware industry is creating a unique challenge for the family violence sector as its products provide perpetrators with new opportunities and possibilities to commit abuse, harassment and intimidation.

Spyware is also being deployed by parents to monitor their children. The consumer spyware industry uses 'parental monitoring' as one of its principal 'legitimate' uses within its marketing material. Head of sales for MSpy, for instance, suggests their customer base is 40% parents monitoring their children and 15% small businesses monitoring employees (with 45% generally unknown or unaccounted for) (Cottle 2014). Spyware however, poses clear risks to article 16 of the *UN Convention on the Rights of the Child* (UNCRC 2018). It offers parents or guardians the capacity to subject children to violating and abusive forms of surveillance.

Furthermore, spyware typically violates the privacy rights of more individuals than its immediate targets. For instance, if spyware is placed within a child's device by a parent, and the child subsequently interacts with other peers through WhatsAPP, Instagram, Facebook Messenger, or via text message or calls, the third-party will also have their private conversation data scooped up by the software (without their consent or knowledge). Spyware has a wide-dragnet that gathers information on more than just the 'target' thus violating the right to privacy of multiple individuals at once.

The nature of the spyware sold by the consumer spyware industry also does not allow the user to tailor which data is scooped from the target-device. Products are generally sold in a package where the target gets the maximum possible data based on the ability of the software to capture various forms of information. Therefore, while the products often advertise themselves as benign 'monitoring' tools, they consistently offer maximal amounts of data-gathering on the target, which outstrips any potential 'legitimate' monitoring application. In this respect, these products support the breaching of the human right to privacy of particular vulnerable groups.

Reinventing regulation and oversight for new technologies

3. How should Australian law protect human rights in the development, use and application of new technologies? In particular:

a) What gaps, if any, are there in this area of Australian law?

Part of the study we are undertaking is purposefully designed to identify the scope and applicability concerning spyware as it relates to Australian criminal and civil law. We look forward to updating the Human Rights Commission with a more detailed legal report involving our work.

In the interim as part of this submission, however, we would like to briefly note some important and pressing dimensions that we have identified thus far. First, a significant concern regarding spyware-related privacy invasions in Australia is the absence of a formal constitutional right to privacy that could protect from privacy-related infringements such as abuse, harassment, and even physical violence.

Furthermore, in instances where harms have already been caused, Australia is further limited in mechanisms for redress that could be remedied through a robust tort of privacy. Relying on breach of confidence for civil matters, while important, is too limiting to address the issue of harms caused through the use of spyware. We regard the introduction of a privacy tort as an essential element in meaningful regulation of harms caused through the use of intrusive and corrosive spyware technologies.

However, as always, the uses and regulation of technology is inextricably connected to social norms that inform behaviours that cause harms. Often, these behaviours are only indirectly connected to questions of 'technology' per se. We insist that any solution to this problem avoid the trap of technological determinism and look toward building healthy relationships of trust and belonging in our communities.

In the coming months, we will update the Human Rights Commission with more detailed results of our legal analysis that addresses issues of: rights of the child, adequacy of Australia's data regulation paradigm under the Privacy Act, as well as further insight into the scope and applicability of existing criminal law such as interception and computer offences, stalking, harassment, and fraud where spyware is involved. We will also update on a range of civil liabilities

and interests involving consumer protection law, intellectual property, the viability of export controls, and other civil matters regarding vendors, platforms, and second party interests.

b) What can we learn about the need for regulating new technologies, and the options for doing so, from international human rights law and the experiences of other countries?

We suggest that any powers to regulate the use of spyware conform with the International Principles on the Application of Human Rights to Communications Surveillance ("Necessary & Proportionate Principles"). We also reiterate our support for the importance of encryption and anonymity tools to the security of persons online, particularly women and children. Proposed measures to weaken or undermine encryption (which includes the purposeful introduction of vulnerabilities into the security and integrity of information communication infrastructure) can pave the way for a net weakening of security that negatively impacts prospects for digital safety online.

c) What principles should guide regulation in this area?

International Principles on the Application of Human Rights to Communications Surveillance ("Necessary & Proportionate Principles") should be a guiding frame for legal, policy, and ethical engagement. Furthermore, states should abide by principles that hold spyware manufacturers more accountable through international coordination. We look forward to updating the Human Rights Commissioner on our academic study into this matter, notably, including steps that can be taken on the basis of a more systematic understanding of criminal and civil liability surrounding the misuse of spyware.

4. In addition to legislation, how should the Australian Government, the private sector and others protect and promote human rights in the development of new technology?

We underscore the importance of multi-stakeholder engagement that furthers education, training, and capacity building for groups that are engaged with harms brought about through forms of technology-facilitated abuse involving spyware. Funding for expert-led training and skills development for non-specialist audiences working in the field of violence against women and children is integral for risk minimisation. Moreover, training and education for law enforcement encountering reports of technology-facilitated violence, and notably spyware, is critical for prioritising a response that works both with and for victims. This is especially the case when it comes to meaningful ways to document digital evidence and provide both sensitive and responsive service.

Artificial intelligence, big data and decisions that affect human rights

5. How well are human rights protected and promoted in AI-informed decision making? In particular, what are some practical examples of how AI-informed decision making can protect or threaten human rights?

[INTENTIONALLY BLANK]

6. How should Australian law protect human rights in respect of AI-informed decision making? In particular:

a) What should be the overarching objectives in regulation in this area?

b) What principles should be applied to achieve these objectives?

c) Are there any gaps in how Australian law deals with this area? If so, what are they?

d) What can we learn from how other countries are seeking to protect human rights in this area?

[INTENTIONALLY BLANK]

7. In addition to legislation, how should Australia protect human rights in AI-informed decision making? What role, if any, is there for:

a) An organisation that takes a central role in promoting responsible innovation in AI-informed decision making?

b) Self-regulatory or co-regulatory approaches?

c) A 'regulation by design' approach?

[INTENTIONALLY BLANK]

Bibliography

Cottle M (2014) The adultery arms race. *The Atlantic.* Available online: https://www.theatlantic.com/magazine/archive/2014/11/the-adultery-arms-race/380794/ (accessed 30th April 2018)

Farrell P (2014) WikiLeaks: NSW police have used hi-tech spyware to monitor Australians. *The Guardian.* Available online: https://www.theguardian.com/uk-news/2014/sep/15/wikileaks-nsw-police-have-used-hi-tech-spyware-to-monitor-australians (accessed 26th April 2018)

Lyons K (2018) Stalkers using bugging devices and spyware to monitor victims. *The Guardian.* Available online: https://www.theguardian.com/uk-news/2018/feb/13/stalkers-using-bugging-devices-and-spyware-to-monitor-victims (accessed 1st May 2018).

Marczak B, Scott-Railton J, and McKune S (2015a) Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware. *The Citizen Lab.* Available online: https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/ (accessed 26th April 2018)

Marczak B, Scott-Railton J, Senft A, Poetranto I, and McKune S (2015b) Pay No Attention to the Server Behind the Proxy Mapping FinFisher's Continuing Proliferation. *The Citizen Lab.* Available online: https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ (accessed 26th April 2018)

McKune S and Deibert R (2017) Who's watching little brother? A checklist for accountability in the industry behind government hacking. *The Citizen Lab.* Available online: https://citizenlab.ca/wp-content/uploads/2017/03/citizenlab_whos-watching-little-brother.pdf (accessed 22nd May 2018)

Re:Charge (2015) *ReCharge: Women's Technology Safety, Legal Resources, Research and Training – National Study Findings 2015.* Available online: http://www.smartsafe.org.au/sites/default/files/ReCharge-Womens-Technology-Safety-Report-2015.pdf (accessed 1st May 2018)

Southworth C (2014) *The Testimony of the National Network to End Domestic Violence with the Minnesota Coalition for Battered Women.* Hearing of the Senate Judiciary Committee Subcommittee on Privacy, Technology and the Law (June 4th 2014). Available online: https://www.judiciary.senate.gov/imo/media/doc/06-04-14SouthworthTestimony.pdf (accessed 22nd May 2018).

UNCRC (2018) *UN Convention on the Rights of the Child.* Available online: https://www.unicef.org.uk/what-we-do/un-convention-child-rights/ (accessed 1st May 2018).

Women's Aid (2018) *Online and digital abuse.* Available online: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/ (accessed 1st May 2018).