2 October 2018

Mr Ed Santow
Australian Human Rights Commission
GPO Box 5218
SYDNEY NSW 2001

By Email: ***tech@humanrights.gov.au***

RE: Submission to the Human Rights and Technology Project

This submission is made jointly by the Australian Privacy Foundation ("**APF**"), the Queensland Council for Civil Liberties ("**QCCL**") and Electronic Frontiers Australia ("**EFA**") in response to the Human Rights and Technology Issues Paper released in July 2018.

The rapid development of technology in the Australia human rights context requires careful consideration as technology can be used for both the benefit and detriment of society. The lack of human rights legislation in Australia makes this consideration particularly important.

The APF, QCCL and EFA appreciate the Commissioner's Issues Paper and the opportunity to provide this submission on this important issue.

We particularly thank the APF's Professional Placement Students, Hannah Taylor and Lauren Jewson, for their assistance in the preparation of this submission.

We trust that this submission is of assistance to the Commission.

Please do not hesitate to contact us to discuss this submission.

Yours sincerely,

……………………
Dr Monique Mann
Board Member, Australian Privacy Foundation
Email: m6.mann@qut.edu.au

……………………
Liam Pomfret
Board Member, Electronic Frontiers Australia and Australian Privacy Foundation
Email: l.pomfret@business.uq.edu.au

……………………
Angus Murray
Vice President, Queensland Council for Civil Liberties
Email: angus@irishbentley.com.au | Phone: 0405 715 427

Australian
Privacy
Foundation

QUEENSLAND COUNCIL FOR
CIVIL LIBERTIES

Electronic
Frontiers
AUSTRALIA

TABLE OF CONTENTS

Executive Summary

This submission has been prepared by the Australian Privacy Foundation, the Queensland Council for Civil Liberties and Electronic Frontiers Australia in response to the Human Rights and Technology Issues Paper released by the Australian Human Rights Commission in July of 2018. The Issues Paper explores the rapid rise of new technology and the resulting impact on human rights.

It is firstly relevant to note that technology is not good or bad – it is a tool. There are examples of positive applications of technology which benefit human rights; such as, for example, increasing the ability for people to observe Court proceedings[1], disseminating information[2], assisting people with disability and increasing the voice of marginalised persons via online forums. However, technology can also be used malevolently, and technology that was created with the best intentions can be manipulated and used oppressively.

It is our submission that many of the concerns contained in this submission *may* be able to be alleviated with an increased focused on human rights education and the introduction of a comprehensive and enforceable federal human rights legislative framework.

The submission is structured to firstly provide an overview of the types of technology that raise human rights concerns. This is followed by an examination of issues that specifically pertain to vulnerable groups and their experiences of new technologies. We then discuss how the Australian law, government, and private sector could better protect privacy in relation to the development, application and use of new technologies. Following this, we discuss the privacy and other human rights concerns raised by algorithmic / artificial intelligence ("**AI**") decision-making.

We conclude with a list of recommendations for the Australian Human Rights Commission to consider in advancing the protection of privacy and other human rights in response to new and emerging technological developments. Our main recommendations are to:

1. Introduce an enforceable charter or bill of human rights at the federal level;

2. Introduce a privacy tort or cause of action for serious invasions of privacy;

3. Improve and increase Australian human rights education at all levels, including schools and workplaces;

4. Release clear and considered guidelines for the development, implementation, application and review of automated decision-making technology with a view to incorporating such provisions into the *Privacy Act 1988* or legislation analogous to the GDPR;

5. Undertake a similar process to the European Parliament's Report with recommendations to the European Commission on civil law rules on Robotics[3];

6. Introduce a Biometrics Commissioner;

[1] Lord Justice Briggs, *Civil Courts Structure Review*: *Interim Report*, (2015) at [45].
[2] See for example: Victoria, *Access to Justice Review*, (2016) at [284].
[3] See: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN.

7. Amend the definition of “personal information” to expressly acknowledge that metadata is capable of being used to identify an individual;

8. Review the *Privacy Act 1988* to ensure it meets international best practice on privacy;

9. Increase funding to the Office of the Australian Information Commission to enable them to undertake their statutory functions;

10. Improve access to justice for privacy disputes by requiring all organisations regulated by the *Privacy Act 1988* to provide access to a free external dispute resolution scheme;

11. Propose ethical technologic creation (including assurances that technology is not built with intentional security weaknesses) and destruction guidelines which incorporate human rights protections;

12. Implement principles of privacy-by-design and data-protection-by-design and default;

13. Recognise that a loss of privacy (as a fundamental and foundational right) has further impacts, for example, the discriminatory impacts of data collection and use targeted towards vulnerable groups and the information security impacts of weakening encrypted form of communication;

14. Acknowledge that the development, creation and disposal of technology has an international environmental and social consequence;

15. Review the scope, manner and extent of human rights education at all levels in Australia; and

16. Encourage and promote Indigenous Data Sovereignty initiatives and associated principles in the collection and use of information concerning Australia’s Indigenous Peoples.[4]

[4] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23), Canberra: Australian National University Press.

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

Our focus in this submission is on *privacy* and how new and emerging technologies can impact the privacy of Australians. This section draws on recent Australian examples including artificial and algorithmic intelligence, CCTV and “Smart CCTV”, robotics and biometric technology.

The collection and use of consumer information has become ubiquitous in the modern, digitally-connected, marketplace and we can reasonably expect that, as data collection, storage and processing capabilities continue to improve, privacy-related issues will only become more significant. The data collected by governments and companies today has many uses, from research to scientific, from criminal to economic. However, in the future, this data could be used for reasons that have not yet been contemplated (or could be contemplated until novel technology has been developed[5]).

Fundamentally, we consider that the issue of consent lies at the heart of the use of technology. Consent can only be considered legitimate if it fully informed, intentional and given wholly voluntarily. Consent should not be sought as a precondition to the use of a service. It must have been explicitly given for specific uses. Individuals must be informed of these intended uses of their information and their consent must carry an obligation for the organisation collecting it to impose these same conditions on any party they may share the information with.

With this basic and reasonable condition in mind, can someone really consent to their data being taken and used for an undefined future purpose or for some purpose which hadn’t even been contemplated at the time it collected the data?

Artificial Intelligence (AI) and Algorithms

Both the concept and definition of artificial intelligence and algorithms are contentious and do not have an agreed definition within the literature. However, to give broad overview we will define these areas and describe their current areas of use. Artificial Intelligence (AI) has been explored in pop culture for decades, suggesting everything from complete destruction to a technological utopia. AI is related to machine learning, in which we give computers incredibly large amounts of data and allow it to ‘learn’ and fill knowledge gaps[6] by sorting information and extrapolating assumptions with varying degrees of certainty.

AI is increasingly an unavoidable part of our daily lives. Algorithms are similar as they use data to make decisions that influence outcomes and judgements. This can be seen simply in platforms like Facebook, Netflix, Google and Amazon which show us different advertisements, or recommend different shows/movies for us to watch. These suggestions are based on what the algorithms “think” that we should enjoy or would be of interest to the individual user. However, it gets more problematic when algorithms start being used to determine mortgage rates or criminal propensity[7] or sway political engagement, as these algorithms are unable to be audited or tested for reliability[8]. This raises significant issues for the protection of human rights.

[5] For example, the Universal Declaration of Human Rights was adopted by the United Nations General Assembly at its third session on 10 December 1948 and it would be difficult to accept that privacy and consumer rights associated with targeting advertising via interconnected search engines which are ubiquitously accessible was contemplated at that time.

[6] Els, A. (2017). “Artificial Intelligence as a Digital Privacy Protector”. *Harvard Journal of Law & Technology*, *31*(1). Retrieved from: http://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech217.pdf.

[7] See for example: *Wisconsin -v- Loomis* 881 NW 2d 749 (Wis 2016).

[8] Els, A. (2017). “Artificial Intelligence as a Digital Privacy Protector”. *Harvard Journal of Law & Technology*, *31*(1). Retrieved from: http://jolt.law.harvard.edu/assets/articlePDFs/v31/31HarvJLTech217.pdf.

The bias that is built into these systems not only reflects the current systematic discrepancies in society but can also exacerbate them by worsening and bolstering unequal treatment.

Social Media

The casual self-disclosures which individuals make in social media have become an important factor in enabling what is effectively ubiquitous surveillance of their daily lives in action. To date, social networking sites have addressed consumer privacy issues through the provisioning of technical tools such as privacy controls and settings. These efforts however are ultimately solutionist, and indicative of a framing of privacy issues that is essentially no different than victim blaming. The presentation of privacy settings as sufficient for consumers to be able to protect their privacy effectively casts privacy as a personal responsibility, ignoring the complex web of interrelated factors that influence these issues. In particular, this framing completely ignores issues relating to institutional privacy that result from the social networking site's own use of consumers' information. This framing of personal responsibility is emblematic of an assumption that rational thinking consumers are free to choose to change their own behaviour.

In the modern digital marketplace platforms such as Facebook have become de-facto infrastructure for the global web. For many, such platforms are both their primary venue for social interaction and their primary source for information about news and current events. Social media usage has become an essential part of peoples' daily lives, and it is not reasonable to expect that consumers' simply cease using social media if they wish to protect their privacy. There is little 'choice' about not using social media if one wants to remain engaged within society. As such, any consent they give on signing up to the service is effectively 'coerced' by the expectations of their social peers.

This business model of social media also raises significant questions about consumer sovereignty and autonomy. Social media represents a new form of marketing power, building on earlier developments in database technologies and electronically mediated communications. These earlier technologies put consumers' ability to author their own identities under threat because of how these identities were ensconced in customer databases. While social networking sites do, to some extent, enable consumers to articulate and tie these identities to their self, social networking users today still do not have direct access and control over these databases. Social media platforms collect and retain information about individual users regardless of whether the user has deleted their account, or even if they never had an account in the first place.

Facebook and other platforms routinely collect data points about people without the direct and explicit consent of the person whose data is being collected. This data comes from a range of sources, including brokers selling customer information, web browsing data from cookies on pages that include social media sharing tools such as Facebook's "like" button, and data from the contact lists of other Facebook users. For example, when an individual allows Facebook access to their list of contacts on their mobile phone (which may be done for the purpose of finding friends who also use Facebook), Facebook collects and retains all of this information. Facebook can then match these details to profiles of existing users, expanding on the information they know about the individual. For instance, while Facebook might already have a phone number for that user, it might not have known the specific email address that was in the contact list uploaded. For any people in the list who Facebook isn't able to match to an existing user, a so-called "shadow profiles" is created for future data matching, despite these people having never given their consent to collection of their personal information, nor having ever agreed to any sort of terms of use. These shadow profiles may even contain biometric data in the form of face recognition data, if a user uploads a photo including the non-user.

Furthermore, these social media companies have an evidenced ability to effect users' emotional state as well as their political views[9]. In our submission, this also creates a significant issue with the right to (informed) political opinion and freedom of speech in addition to the right not to be subjected to arbitrary interference into privacy, family, home or correspondence.

Online Compliance Intervention (RoboDebt)

In July 2016 the Department of Human Services, via Centrelink, launched an online debt raising and recovery program that automatically matched earnings reported on clients records to annual income recorded by the Australian Taxation Office.[10] In comparing these data sources, an algorithm identified discrepancies that were meant to identify 'over-payments' of social security benefits.

Within the first three (3) months of the program over 230,000 letters were sent to Centrelink clients seeking repayment for debt[11] at a rate of around 20,000 debt notices being issued every week.[12] It is estimated that around 20-38% of the debt letters issued were incorrect,[13] as a direct consequence of removing the human oversight of the process. In essence, the program resulted in the use of mismatched and inaccurate data to target thousands of welfare recipients and a lack of fair processes enabling clients to have their debt notice reviewed.[14] A subsequent parliamentary inquiry recommended suspending the system until issues of procedural justice (i.e. errors in matching, data inaccuracies and avenues for review of automated decisions) were addressed.[15]

While this relates to areas of administrative justice, the control (and correction) of personal information is of significant concern. It also raises the issue that we have few controls over automated decision-making.

The Australian *Privacy Act 1988* (Cth) would benefit from similar limitations on automated decision-making and profiling as contained at Art. 22 of Regulation (EU) 2016/679 (General Data Protection Regulation) ("**the GDPR**"). Although we accept that the GDPR isn't perfect, it does begin to try to clarify the 'right to explanation'. However, the issues are that there are barriers to the understanding of these algorithms even with a 'right to explanation'.

The first is that companies may try to intentionally conceal how decisions are made to avoid public scrutiny or scrutiny from competitors. Secondly, most people wouldn't be able to understand the coding of the algorithm if it was given to them, so it would need to be explained rather than merely presented in its basic format. Thirdly, the difference between the mathematical way that computers make decisions and predictions, and how people

[9] Fick, C (2016) "Informed consent and the Facebook emotional manipulation study" Sage Journal Volume 12, issue 1 at pages [14] – [28]. Retrieved from: http://journals.sagepub.com/doi/full/10.1177/1747016115599568.

[10] Glenn, R. (2017). *Centrelink's automated debt raising and recovery system: A report about the Department of Human Services' online compliance intervention system for debt raising and recovery*. Brisbane, QLD: Commonwealth Ombudsman. Retrieved from: https://www.ombudsman.gov.au/__data/assets/pdf_file/0022/43528/Report-Centrelinks-automated-debt-raising-and-recovery-system-April-2017.pdf.

[11] Anonymous. (n.d.). *The issue*. #NotMyDebt. Retrieved from: https://www.notmydebt.com.au/the-issue.

[12] Ibid.

[13] Ibid.

[14] Galloway, K. (2017). Big data: A case study of disruption and government power. *Alternative Law Journal* 42(2), 89-95.

[15] Community Affairs References Committee (2017). *Senate inquiry into the design, scope, cost-benefit analysis, contracts awarded and implementation associated with the Better Management of the Social Welfare System initiative*. Canberra: Commonwealth of Australia.

make decisions and interpretations based on data.[16] The fourth is that algorithmic decision making may be protected by intellectual property law and/or trade secret which creates barriers to transparent decision making and due process.

We submit that RoboDebt ought to serve as an example on the complexities and difficulties with implemented automated decision-making technology and that the Commissioner ought to release clear and considered guidelines for the development, implementation, application and review of automated decision making with a view to incorporating such provisions into the *Privacy Act 1988* or analogous legislation to the GDPR that ought to be introduced in Australia.

CCTV

Despite CCTV being justified in most cases as a technique of crime prevention, studies have shown that visual surveillance fails to prevent certain types of crime[17]. A systematic review of CCTV cameras found that they are most effective at preventing crime in car parks, related to theft from or of vehicles[18]. However, it has been found that CCTV struggles to have an impact on the prevalence of violent crime.[19] CCTV systems instead can discourage citizens from exercising their fundamental rights, especially those belonging to minority groups or those suffering from the stigma of being an outsider.[20]

The positioning of CCTV cameras can have a severe impact on professional secrecy. If a camera is positioned in the visual range of doors and windows of certain offices and institutions which maintain a level of professional secrecy, this can be breached by the use of CCTV cameras[21]. All data is vulnerable to misuse and unauthorised access, but the if the data recorded by CCTV systems is breached, the threat to privacy becomes severe. It is essential that CCTV systems are secure.[22] It is essential that safeguards are utilised to prevent further privacy concerns for individuals as a result of data leaks or breaches.[23] The privacy infringements that result from CCTV systems struggle to be accepted due to their failure to prevent crimes and negative impact on the lives of innocent civilians.[24]

Robotics

Robotics are utilised throughout various aspects of society and will continue to be utilised in many different ways into the future. However, despite the potential advantages provided by the use of robotics, there are also privacy risks. Robots are defined as having agency and currently a degree of autonomy, they can collect, process and to a limited degree affect the world around them[25]. Robotics are already utilised as a method of surveillance, as

[16] Goodman, B. and Flaxman, S. (2016). “European Union regulations on algorithmic decision-making and a ‘right to explanation’”. *ICML Workshop on Human Interpretability in Machine Learning*, arXiv:1606.08813 (v3); (2017) 38 AI Magazine 50.

[17] Schlehahn, E, Hansen, M, Sterbik-Lamina, J. (2013). Report on surveillance technology and privacy enhancing design. *SurPRISE Project.* http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf

[18] Welsh, B. and Farrington, D. (2008). “Effects of closed circuit television surveillance on crime.” *Campbell Corporation*. Retrieved from: https://campbellcollaboration.org/library/effects-of-closed-circuit-television-surveillance-on-crime.html.

[19] Cayford, M & Pieters, W (2018) The effectiveness of surveillance technology: What intelligence officials are saying, *The Information Society, 34(2),* 88-103. DOI: 10.1080/01972243.2017.1414721

[20] Ibid.

[21] Schlehahn, E, Hansen, M, Sterbik-Lamina, J. (2013). Report on surveillance technology and privacy enhancing design. *SurPRISE Project.* http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf

[22] Schlehahn, E, Hansen, M, Sterbik-Lamina, J. (2013). Report on surveillance technology and privacy enhancing design. *SurPRISE Project.* http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE-D3.1-Report-on-surveillance-technology-and-privacy-enhancing-design.pdf

[23] Ibid.

[24] Möllers, N & Hälterlein, J. (2013) Privacy issues in public discourse: the case of “smart” CCTV in Germany. *Innovation: The European Journal of Social Science Research, 26(1-2),* 57-70. DOI: 10.1080/13511610.2013.723396

[25] Ibid.

exemplified by drone spying in military contexts,[26] but there is opportunity that more domestic robotic technology could be utilised in the same way. Robots used within the home, such as for healthcare, could be utilised for surveillance purposes by the government, corporations or private citizens.[27] In this situation, a harmless robot purchased by the surveillance subject can be hijacked by the government to monitor their whereabouts and habits and relay the information back to the government.[28]

As a result of their vital role in some industries, robots have extensive access to personal information. For social robots used within the healthcare context, identifiable user data (e.g. names, date of birth, food preferences) is collected to allow the robot to analyse and act upon the vast body of data.[29] This access to a wide array of data raises privacy concerns, such as the security of the data, and the transparency surrounding other uses for the data. As humans have a tendency to bond with robots in a similar way to other humans, individuals can be inclined to discuss very personal and delicate topics with robots.[30] In these situations, however, the robot may not be designed to deal with sensitive topics adequately, raising both informational and physical privacy concerns. As robotics continue to develop and become further integrated within society, it is certain that further privacy concerns will be uncovered.

We respectfully submit that it would be appropriate for the Commission to undertake a similar process to the European Parliament's Report with recommendations to the European Commission on civil law rules on Robotics[31].

Drones and Unmanned Aerial Vehicles (UAVs)

The continued advancement of drones allows for increased visual surveillance as smaller drones become capable of carrying remotely controlled cameras.[32] Drones allow for more intensive surveillance to take place as the perspective of the observation is from above, and the drone is easily manoeuvrable allowing for quick point of view change and the ability to pursue a surveillance target.[33] Drones can be used for many reasons from environmental monitoring to observation of construction to wildlife tracking. However, it can also be used by law enforcement and national security agencies for border watching, as well as observation of criminals and of demonstrations.[34]

There has also been an increase in civilian drone ownership, as the economic constraints are much lower, and this increase in usage results in further difficulties in enforcing laws that seek to protect privacy.[35] In recent years, there have been many incidents of drones "spying" on neighbours in residential areas,[36] further demonstrating the privacy concerns that result from drone technology. Drones increase the ability of visual surveillance, not only for law enforcement agencies and the military but also for civilians.[37] They increase the level of invasiveness, as they are able to observe more, transit more, record more and more easily

[26] Lutz, C, Tamò, A. (2016). *Privacy and Healthcare Robots – An ANT Analysis. https://pdfs.semanticscholar.org/1e27/5833c92e2276e09c6f16761191ad5ddab979.pdf*
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Ibid.
[31] See: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN.
[32] Australian Privacy Foundation *Drones* (March 2014) https://privacy.org.au/policies/drones/.
[33] Ibid.
[34] Clarke, R. (2014). "The regulation of civilian drones' impacts on behavioural privacy." *Computer Law and Security Review* 30 (2014). Retrieved from: https://doi.org/10.1016/j.clsr.2014.03.005.
[35] Ibid.
[36] See: Gogarty, B. (2017, April 26th). Backyard skinny-dippers lack effective laws to keep peeping drones at bay, *ABC News.* Retreived from: http://www.abc.net.au/news/2017-04-26/peeping-drones-backyard-skinny-dippers-and-the-law/8472446.; Box, G. (2018, May 25th). Mums raise privacy alert over drones in backyards, *The West Australian.* Retrieved from: https://thewest.com.au/news/mid-west/mums-raise-privacy-alert-over-drones-in-backyards-ng-b88840233z.
[37] See also: https://qccl.org.au/wiki/angus-murray-speech-to-the-constitutional-convention-in-cairns/.

track the location of an individual.[38] This is a large privacy issue due to the lack of legislation in Australia that not only regulates the use of drones and UAVs but also protects the privacy of those affected by these machines.

Biometric technology

In late 2015, via an agreement made by the Council of Australian Governments ("**COAG"**), the Commonwealth government implemented a national facial recognition system—the National Facial Biometric Matching Capability, or simply the Orwellian sounding 'Capability.' This system uses first generation biometrics to identify an individual using existing identification documents, such e-passports, to extract and share biometric information between government databases.

In 2018, the Government introduced two bills to respond legislatively to the activities already sanctioned under COAG agreements and in an attempt to obtain access to all state and territory driver license or roads traffic authority databases. This included the *Identity-matching Services Bill 2018* (Cth) which will authorise the Department of Home Affairs to collect, use and disclose identification information in order to operate the systems that will support a set of new biometric face-matching services and also the *Australian Passports Amendment (Identity-matching Services) Bill 2018* (Cth) will authorise the Minister for Foreign Affairs to disclose personal information for the purpose of participating in a service to share or match information relating to the identity of a person.

The *Identity-matching Services Bill 2018* (Cth) allows information to be collected about individuals who have not been convicted of a crime, which is considered neither a legitimate nor proportionate invasion of privacy and is at odds with precedent set by the European Court of Human Rights in *S & Marper*.[39]

There are several issues and concerns associated with the collection, sharing and use of biometric information including that they are extraordinarily privacy-invasive, highly error-prone and unreliable and discriminatory.[40] It also brings under a central federal authority, tasked with policing, migration, intelligence the richest datasets of personal information previously held at state level. Due to the limited protections in relation to biometrics information in Australia (which is defined under the Australian Privacy Principles as 'sensitive information'), and the numerous exemptions and carve outs in the *Privacy Act 1988* (Cth) as discussed above, there is a significant gap in proper governance and oversight.[41]

There are also various issues raised by both first- and second-generation biometrics. We have already mentioned first generation biometrics above, so this section will focus on second generation biometrics. Second generation biometrics uses behavioural monitoring to try and prevent criminal activity and hostile actions[42]. This type of behavioural monitoring, uses body movement, gait while walking, body heat, heart rate and public activities to make predictions. As mentioned below "Smart CCTV" can now be used to capture these biometrics from a distance, which allows this surveillance to be done without the knowledge or consent of the subject. This opens the door to higher levels of marginalisation and discrimination if the predictions made by the biometrics are wrong, which currently has a

[38] Ibid.

[39] Galloway, K., Mann, M., & Goldenfien, J. (2018). Submission to the Parliamentary Joint Committee on Intelligence and Security: Review of the Identity-matching Services Bill 2018 and the Australian Passports
Amendment (Identity-matching Services) Bill 2018. *FutureWise and the Australian Privacy Foundation.* Retrieved from: https://eprints.qut.edu.au/116911/1/FW_APF_BiometricSubmission_Final.pdf.

[40] Ibid.

[41] Mann, M., & Smith, M. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *University of New South Wales Law Journal, 40(1), pp. 121-145.*

[42] Sutrop, M. & Laas-Mikko, K. (2012.) "From Identity Verification to Behavior Prediction: Ethical Implications of Second Generation Biometrics." *Review of Policy Research* 29 (1), 21–36. DOI: 10.1111/j.1541-1338.2011.00536.x.

high chance of happening.[43] The next question we must ask is what the future of biometrics holds for the privacy rights of the Australian population considering the ethical issues that are currently plaguing biometrics.

Currently, Australia's regulations do not align with international regulatory practices, such as those in the United Kingdom which has a dedicated Biometrics Commissioner.[44]

By introducing a Biometrics Commissioner[45], the regulatory agency would ensure the Australian government and private sector are effectively and conclusively protecting the human rights of all citizens in regards to the use of biometric technology. As the right to privacy is a foundational right, the introduction of a Biometrics Commissioner would allow biometric technology to be utilised throughout Australia whilst providing an oversight body that ensures the application of biometric technology consistently maintains the human right to privacy for all citizens.

We submit that a Biometrics Commissioner ought to be appointed in Australia.

"Smart" CCTV

Traditional closed-circuit television ("**CCTV**") systems have been significantly advanced in recent years with the introduction of new "Smart CCTV". The advanced systems utilise algorithms to automatically detect events of interest and notify the operator.[46] This use of algorithms removes the need for constant monitoring,[47] but also leaves the system vulnerable to problems of false positives and negatives, as witnessed in the RoboDebt incident discussed above.

In America, CCTV images are being assessed against driver's license photos and mugshots without the consent of the subjects. The problem is that CCTV and these algorithms that find matches are discriminatory, as facial recognition technology disproportionately affects African-Americans. The second problem is that there is research to suggest that facial recognition is also less accurate when looking at African-Americans.[48]

In Australia, the Toowoomba Regional Council has implemented a trial of new facial recognition technology that is used to analyse images recorded by existing CCTV cameras.[49] The use of this biometric technology is concerning as it allows for CCTV-enabled tracking through public places, and can be integrated with other big data utilised for law enforcement and security purposes.[50] A similar facial recognition surveillance initiative is also being implemented in Perth suburbs, used to detect known "troublemakers" and people wanted by police.[51] In addition to CCTV initiatives, Victorian Police have introduced drones that have biometric monitoring capabilities, designed to help police identify 'irregular' behaviour.[52] The use of these biometric surveillance techniques raises many concerns due

[43] Ibid.
[44] Ibid.
[45] See for example: The Crown. (2018). Biometrics Commissioner. *GOV.UK.* Retrieved from: https://www.gov.uk/government/organisations/biometrics-commissioner.
[46] Möllers, N & Hälterlein, J. (2013) Privacy issues in public discourse: the case of "smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research, 26(1-2),* 57-70. DOI: 10.1080/13511610.2013.723396
[47] Ibid.
[48] Garvie, C., Bedoya, A. and Frankle, J. (2016). "The Perpetual Line-Up." Georgetown Law: Center on Privacy and Technology. Retrieved from: https://www.perpetuallineup.org/
[49] Guest, A. (2017 March, 10). Facial recognition software trials in Queensland alarm privacy advocates. *ABC News.* Retrieved from: http://www.abc.net.au/news/2017-03-08/facial-recognition-software-trials-in-qld-alarm-privacy-advocate/8335142
[50] Ibid.
[51] Campbell, K. (2018 July 29). Facial recognition CCTV: East Perth residents wary over spy cameras. *Perth Now.* Retrieved from: https://www.perthnow.com.au/technology/security/facial-recognition-cctv-east-perth-residents-wary-over-spy-cameras-ng-b88910065z.
[52] ABC News (2018, September 19). Drones hovering over crowds the future for police anti-terror strategies. *ABC News.* Retrieved from: http://www.abc.net.au/news/2018-09-19/victoria-police-new-anti-terrorism-bid/10280484.

to the significant invasion of privacy that results from the application of this “smart” technology.

Genomics

Recognition in business, government and academia about the potential for genomic research to address intractable questions regarding public health and foster personalised (aka precision) medicine – evident in large-scale funding of initiatives such as the Genomics Health Futures Mission – has not been matched with awareness of and respect for privacy concerns.[53] Genomic technologies have an intergenerational privacy dimension, given that genomic data is substantially common to blood relatives and that big data applications facilitate the re-identification of ostensibly robustly de-identified data. There is a need for community education, enhanced capability on the part of regulators at the state/territory and Commonwealth levels, and forward-looking law reform that for example encompasses consumer protection regarding offshore recreational genomics services.[54]

Databases and Information Collection, Centralisation and Sharing

Recently, various information sources and technologies have begun to be integrated. There are some strong privacy implications of this, especially in regard to re-identification and data linkage. In September 2016, a team of researchers from Melbourne University[55] found that it was possible to re-identify practitioner details within a research dataset the Department of Health had placed in its open data portal, based on a 10% sample of the national Medicare payments data set including data derived from both doctors and patient transactions[56]. Data linkage is also a large issue because of its all encompassing nature and how it permeates all aspects of our lives. As the name suggests, data linkage tries to link together all of the data from one person to create a more holistic view of an individual. However, this raises the issues of privacy when this data linking is done without consent.

CensusFail and the creation of Statistical Linkage Keys

In December 2015, the Australian Bureau of Statistics (“**ABS**”) announced that the 2016 Census would involve the collection and retention of names and addresses to “enable a richer and dynamic statistical picture of Australia”.[57] This would differ to previous administrations of the census where this information was not required. The ABS would then use this information to create a ‘statistical linkage key’ (“**SLK”**) that enables data linkage and longitudinal tracking creating a detailed picture of every Australian resident.[58]

Each of the APF, QCCL and EFA made submissions to the Senate Inquiry following the 2016 Census regarding various privacy issues.[59] The changes to the Census and the creation of SLKs change this data collection exercise from statistical data collection to

[53] Arnold, B. & Bonython, W. (2018) Not As Good As Gold: Genomics, Data and Dignity in Day, A., Devitt, K. & Mann, M. (eds) Good Data Amsterdam: *Institute of Network Cultures*.

[54] Bonython, W., & Arnold, B. (2015) Personhood, and Property in the Age of Genomics, *Laws* 4.3 pp 377-412.

[55] Namely being: Vanessa Teague, Chris Culnane and Ben Rubinstein.

[56] Culnane, C., Rubinstein, B., & Teague, V. (2016, September 29th). Understanding the maths is crucial for protecting privacy, *Pursuit.* Retrieved from: https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy.

[57] Australian Bureau of Statistics. (2015, December 18th). *Retention of names and addresses collected in the 2016 Census of Population and Housing.* Canberra, ACT: Australian Government. Retrieved from: http://www.abs.gov.au/websitedbs/D3310114.nsf/home/Retention+of+names+and+addresses+collected.

[58] Australian Privacy Foundation. (2016). The problems with the 2016 Census, *Australian Privacy Foundation*. Retrieved from:https://privacy.org.au/campaigns/census2016/.

[59] See: Galloway, K., Mann, M., & Goldenfien, J. (2018). *Joint submission to the Parliamentary Joint Committee on Intelligence and Security:* Review of the *Identity-matching Services Bill 2018* and the *Australian Passports Amendment (Identity-matching Services) Bill 2018.* Canberra: Australian Government. Retrieved from:https://eprints.qut.edu.au/116911/1/FW_APF_BiometricSubmission_Final.pdf.

individual tracking and surveillance.[60] This constitutes a significant breach of public trust and social license to operate, especially since there was inadequate consultation with the public or civil society.

Mandatory Metadata Retention

In 2015, the Australian Government amended the *Telecommunications (Interception and Access) Act 1979 (Cth)* to introduce a statutory obligation for telecommunication and internet service providers (ISPs) to retain the metadata of their subscribers for a period of two years.[61] The retention of individuals' data who have no connection to any investigations concerning serious crime or national security is unnecessary and the government would be better served utilising targeted investigation techniques.[62]

This amendment grants law enforcement and security agencies the ability to request access to an individual's metadata without a judicial warrant.[63] Agencies who have access to this data include Australian Security Intelligence Organisation (ASIO), Australian Federal Police (AFP), and any other federal, state and territory agencies.[64] Initially there were over 60 agencies (many not concerned with matters of national security or law enforcement) that could access this information. This was then restricted to enforcement agencies, although there has been evidence of agencies funnelling requests to authorised agencies and then subsequently informally sharing the information to circumvent this restriction.[65]

While described as assisting law enforcement and national security efforts,[66] there is also particular concern with the data retention regime regarding the ability for agencies to access the metadata of journalists.[67] Indeed, the Australian Federal Police, by their own admission, accessed the data of a journalist without warrant (as the legislation introduced a 'safeguard' of journalist information warrants requiring law enforcement to obtain a warrant before accessing journalists' metadata). This highlights that there is not only the potential for, but actual, abuse of the data retention system. Further, there are insufficient oversight and accountability mechanisms to ensure that this does not occur.

Australia's data retention laws are in direct conflict the Court of Justice of the European Union ruling in the *Digital Rights Ireland* case that struck down the Data Retention Directive in the EU. The retention of metadata represents a disproportionate interference with individual rights and is at off with international precedent.[68] The law enables agencies to create a comprehensive digital picture of individuals' movements, contacts, interests and

[60] Australian Privacy Foundation. (2016). Inquiry: Census 2016, *Australian Privacy Foundation.*Retrieved from:https://privacy.org.au/Papers/Sen-Census-160927.pdf.

[61] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015 (Cth)* (Austl.). Retrieved from: https://www.aph.gov.au/Parliamentary_Business/Bills_LEGislation/Bills_Search_Results/Result?bId=r5375.

[62] Linsay, D. (2015). *Submission to the Inquiry into Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015.*Retrieved from:https://privacy.org.au/Papers/PJCIS-DataRetention-150119.pdf; Lane, K., Lindsay, D., & Vaile, D. (2016). *Submission to Review of Access to Retained Data in Civil Proceedings.* Australia: Australian Privacy Foundation. Retrieved from:https://www.ag.gov.au/Consultations/Documents/Access-to-telecommunications-data/Australian-Privacy-Foundation.DOCX

[63] Sarre, R. (2017). Metadata retention as a means of combating terrorism and organised crime: A perspective from Australia, *Asian Journal of Criminology, 12*(3), 167-179. Retrieved from:https://link.springer.com/article/10.1007/s11417-017-9256-7.

[64] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2015*(Cth) (Austl.)

[65] Mann, M et al. (2018). The limits of (digital) constitutionalism: Exploring the privacy- security (im)balance in Australia, *The International Communication Gazette 80 (4), 369–384. Retrieved from:*https://doi-org.ezp01.library.qut.edu.au/10.1177/1748048518757141.

[66] Ibid.

[67] Royes, L. (2017, April 29th). AFP officer accessed journalist's call records in metadata breach, *ABC News.* Retrieved from: http://www.abc.net.au/news/2017-04-28/afp-officer-accessed-journalists-call-records-in-metadata-breach/8480804; Suzor, N., Pappalardo, K., & McIntosh, N. (2017). The passage of Australia's data retention regime: National security; human rights, and media scrutiny, *Internet Policy Review, 6*(1), 1-16.

[68] Lane, K., Lindsay, D., & Vaile, D. (2016). *Australian Privacy Foundation: Submission to Review of Access to Retained Data in Civil Proceedings.*Australia: Australian Privacy Foundation.

associations.[69]. In the most recent ruling in *Big Brother Watch v UK*[70] in European Court of Human Rights, it was found that metadata is just as important as the actual communications content in relation to right for privacy. Metadata can be used to identify a person (sender or receiver), their location and other identifying information.[71]

We respectfully submit that the definition of "personal information" ought to be amended to expressly acknowledge that metadata is capable of being used to identify an individual.

Attempts to undermine encryption[72]

Former Prime Minister Malcolm Turnbull announced plans to limit the use of encryption by putting the onus on domestic and offshore technology companies to assist law enforcement and security agencies to access information (the 'not-a-backdoor' *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*).[73] Former Attorney-General Brandis stated that encryption was "*going to degrade if not destroy our capacity to gather and act upon intelligence*" as "*within a short number of years, effectively 100% of communications are going to use encryption*."[74] Following this logic, the Australian Government has recently introduced a draft of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (14th August 2018).

The *Assistance and Access Bill 2018* aims to facilitate a partnership between law enforcement agencies and the communications industry, to ensure law enforcement agencies can access data. For example, the Bill allows the Director-General of Security or the chief officer of an interception agency to compel a provider to do an unlimited range of *acts or things*. That could mean anything from removing security measures to deleting messages or collecting extra data. Providers will also be required to conceal any action taken covertly by law enforcement. Further, the Attorney-General may issue a technical capability notice *directed towards ensuring that the provider is capable of giving certain types of help* to ASIO or an interception agency.

This means providers will be required to develop new ways for law enforcement to collect information. Following the release of the draft *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018*, Greens Senator Jordon Steele-John expressed concern by stating "installing software or legislating some other means to capture data as it is unencrypted on the receiving device undermines the very principle of end-to-end encryption".[75] However, as the Bill would trigger penalties for refusing to provide data to government agencies or leaking information about government activities, there are significant issues regarding transparency and accountability of these government agencies.[76]

[69] Sarre, R. (2017). Metadata retention as a means of combating terrorism and organised crime: A perspective from Australia, *Asian Journal of Criminology, 12*(3), 167-179. Retrieved from: https://link.springer.com/article/10.1007/s11417-017-9256-7.
[70] See: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-186048%22]}.
[71] Burgess, K. and Islam, T. 2018. "Unpacking Big Brother Watch v UK." *International Association of Privacy Professionals.* Retrieved from: https://iapp.org/news/a/unpacking-big-brother-watch-v-uk/.
[72] See Joint Civil Society submission to the Department of Home Affairs dated 10 September 2018 located at: https://digitalrightswatch.org.au/2018/09/11/submission-to-home-affairs-on-the-assistance-and-access-bill-2018/.
[73] Mann, M, Molnar A, and Daly, A. (2018). Undermining encryption won't work, and police have enough powers anyway. Retrieved from: https://www.policyforum.net/undermining-encryption-wont-work-police-enough-powers-anyway/.
[74] Wroe, D. (2017, June 11th). How the Turnbull government plans to access encrypted messages, *The Sydney Morning Herald.* Retrieved from: https://www.smh.com.au/politics/federal/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html.
[75] Sarraf, S. (2018, August 14th). Federal Govt. releases proposed reform to access encrypted communications, *ARN*. Retrieved from: https://www.arnnet.com.au/article/645175/federal-govt-releases-proposed-reform-encryption-laws/.
[76] Mann, M. (2018, August 15th). The devil is in the detail of government bill to enable access to communications data, *The Conversation*. Retrieved from: https://theconversation.com/the-devil-is-in-the-detail-of-government-bill-to-enable-access-to-communications-data-96909.

This approach is modelled on the UK approach in the *Investigatory Powers Act 2016* (UK). The legislation in the UK and Australia's proposed bill stipulate that communications companies provide assistance to law enforcement, when compelled to do so. For example, section 253 of the UK's *Investigatory Powers Act 2016*, on 'technical capability notices' provides that the Government minister, subject to approval by a 'Judicial Commissioner', can issue a communications operator with a notice which can oblige the operator to remove 'electronic protection applied by or on behalf of that operator to any communications or data'. Similarly, Australia's *Assistance and Access Bill 2018* establishes three levels of assistance[77] that can be sought by law enforcement personnel.[78] The third and most extreme level mirrors the UK legislation and stipulates that communications companies must build capabilities in order to assist law enforcement agencies. However, the Director-General of Security, the chief officer of an interception agency and the Attorney-General can issue notices without judicial oversight. This differs from how it works in the UK, where a specific judicial oversight regime was established, in addition to the introduction of an Investigatory Powers Commissioner.

At present, it is not clear whether a provider receiving a technical capacity notice would be able to provide true end-to-end encryption for its customers in the first place, in order to ensure that the provider has a means of decrypting communications.[79]

This is concerning because encryption tools are essential to protect individual privacy and critical digital infrastructure. Any attempt to weaken or undermine strong encryption poses serious risks to both information security and privacy. The nature of the powers set out in the Bill are so broad in potential application that they undermine trust in all range of digital services and opens up the potential for abuse and misuse. A previous joint submission to the Government with regards to the *Assistance and Access Bill 2018*, has made clear that we, and a large number of other civil society organisations, are extremely concerned about the consequence of this legislation being passed in general but particularly in circumstances where human rights are not presently adequately protected in Australia.

In this regard, the issues with the *Assistance and Access Bill 2018* are broadly and generally that; firstly, with the broad scope (seemingly scopeless) definition of "designated communication providers". Secondly, the increase of obligations on communication providers to assist with law enforcement agencies. Thirdly, it introduces covert computer access warrants enabling law enforcement to search computers and electronic devices without an individual's knowledge. And lastly, it increases the powers of law enforcement to use and apply the currently available search and seizure warrants.

My Health Record (MyHR)

My Health Record (MyHR) is an online database of sensitive medical data established by the Australian Government that collects summary health information for all Australians who do not opt-out. There are various issues with My Health Record including the government changing the system from 'opt-in' (requiring consent to gather and share health data) to one that requires Australians to 'opt-out' during a four (4) month period beginning 16 July 2018.[80]

[77] The first level is a "technical assistance request" which denotes voluntary assistance by a communications company. The second level is a "technical assistance notice" that compels a communications company to offer assistance that is within the bounds of their resources (e.g., decrypting data using a key already in the provider's possession).

[78] Pearce, R. (2018, August 14th). New law to force tech companies to build features for police, *Computerworld.* Retrieved from: https://www.computerworld.com.au/article/645174/new-law-force-tech-companies-build-features-police/.

[79] Smith, G (2017b). Squaring the circle of end to end encryption. *Cyber Legal Eagle*. Retrieved from: https://www.cyberleagle.com/2017/05/squaring-circle-of-end-to-end-encryption.html.

[80] Australian Privacy Foundation. (n.d.) *My health record: what is it, and why should I care?*Australia: Australian Privacy Foundation.

After the end of the 'opt-out' period only newborns or new citizens will be permitted to opt-out.

There is a disturbing lack of control in relation to which health professionals can gain access to private medical data and default privacy settings. The default setting is that health professionals decide whether they should have access to private information meaning that by default, all data in a record is viewable by all health professionals. The only stipulation is that it is part of the health care of the patient. How this is to be policed is unclear. Many patients will not have the capability to monitor who has accessed their health record, something that is particularly difficult to do because the logs do not show which individuals have accessed a record, only which institutions. More alarmingly, this information can also be accessed by a wide range of non-health related agencies. For example, police and other non-health professionals can access records[81] in situations such as preventing or investigating crime and 'protection of public revenue.'

The government has announced that it intends changing the law such that a court order is required by these agencies to access a My Health Record, but it will still be without the consent of the patient. It is important to realise that the data in My Health Record is intended to be downloaded to other systems where the legislative protections of the system no longer apply. The My Health Record system is part of a larger environment of medical data with varying degrees and levels of access control and visibility to patients, most of which are unclear to patients and health professionals alike.

The 'Trusted' Digital Identity Framework

The Data Transformation Agency ("**DTA**") is responsible for leading the development of a national federated digital identity system, knowns as the Trusted Digital Identity Framework ("**TDIF**").[82] In essence, this is an online identity system that is governed by a set of rules used to manage identity transactions.[83] The Australian government intends that the TDIF will form the basis of a federated system known as 'Govpass,' which will serve as a "one stop shop" for identity confirmation and access to online government services.[84] Govpass requires individuals to prove their identity in order to access a range of government services.[85] The Govpass system will be accessed by the user through the new Facial Identification Service (as part of 'The Capability' as described above), which requires an individual to take and upload a 'selfie'[86] which will then be compared to a passport or drivers license photo to confirm identity.[87]

This mechanism will serve as the first part of a two-factor authentication process, the second being a code sent to either an email address or a phone number. The DTA have not yet discussed how they plan to ensure the photo taken by the website is live, or not a printed photo, but these possibilities raise obvious concerns as regards to the security of users' information. The DTA claims that privacy and the protection of personal information is at the

[81] *My Health Records Act 2012*(Cth) (Austl.)

[82] Digital Transformation Agency. (2018). *Overview and Glossary: Trusted Digital Identity Framework February 2018, version 1.0.* Canberra, ACT: Australian Government. Retrieved from:https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-overview-and-glossary.pdf.

[83] Ibid.

[84] Digital Transformation Agency. (n.d.). *Govpass*. Canberra, ACT: Australian Government. Retrieved from:https://www.dta.gov.au/what-we-do/platforms/govpass/.

[85] Ibid.

[86] Digital Transformation Agency. (2018). *Identity Proofing Requirements: Trusted Digital Identity Framework February 2018, version 1.0.* Canberra, ACT: Australian Government. Retrieved from:https://dta-www-drupal-20180130215411153400000001.s3.ap-southeast-2.amazonaws.com/s3fs-public/files/digital-identity/tdif-identity-proofing-requirements.pdf.

[87] Ibid.

“heart of this project”[88] but despite these reassurances there still remains serious concern about data retention and access.

The issue with the large amount of data collected and stored is that this data, no matter how well protected will be a “honeypot” for hackers who would either use the information for identity theft or sell it on to the highest bidder. Also, the data collected isn’t just “metadata”, it is a basic description of your life. If you need to call a specialist doctor, like an obstetrician or an oncologist, the content of the conversation does not need to be heard to conclude the meaning of the call. Another example is calling a suicide hotline, or a psychologist’s office, or a domestic violence hotline or a women’s shelter. Metadata not only includes who you call, but also how long you speak for and an approximate location of where you called from. This information is then kept and stored for two (2) years. This represents an unjustified intrusion into everyday Australian’s lives.

The Creation and Disposal of Technology

We also submit that it is important to consider that technology is often manufactured and destroyed in foreign countries where human rights violations are rife[89].

We respectfully submit that the Commissioner ought to propose ethical technologic creation (including assurances that technology is not built with intentional security weaknesses) and destruction guidelines which incorporate human rights protections.

Question 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)?

Experiences of New Technology by Vulnerable and Marginalised Groups

In order to function independently within society, it is necessary to have some interaction with technology as technology is heavily relied upon in all aspects of life, from banking to home security[90]. This use of technology poses challenges for particular groups within the Australian Community, as differing experiences of new technology influence the ability for individuals to effectively engage with new trends.

Vulnerable and marginalised groups, such as children and young people, women, the elderly, racial and ethnic minorities, LGBTQIA+ individuals and immigrant populations, have different experiences of new and emerging technology and privacy issues[91]. This is a significant focus because of the consequences of being in a vulnerable group. Vulnerable groups have less agency compared to other more powerful parts of society and they have more issues with challenging the status quo. Vulnerable and marginalised groups are more affected by wider issues such as privacy and data collection because of their difference in status. Below, we cover some of the vulnerable and marginalised groups and various programs within Australia that negatively affect them and their privacy.

[88] Digital Transformation Agency. (n.d.). *Govpass*. Canberra, ACT: Australian Government. Retrieved from:https://www.dta.gov.au/what-we-do/platforms/govpass/.

[89] See for example: https://www.theguardian.com/global-development/2017/dec/02/chittagong-shipbreaking-yards-legal-fight.

[90] Czaja, Sara & Lee, Chin. (2006). The impact of aging on access to technology. *Universal Access in the Information Society*, 5(4), pp.341–349. DOI 10.1007/s10209-006-0060-x

[91] Linabary, J. and Corple, D. (2018). “Privacy for whom?: A feminist intervention in online research practice.” *Information, Communication and Society*. Retrieved from: https://doi.org/10.1080/1369118X.2018.1438492.

Children and Young People: Surveillance in Schools

One of the larger areas that technology has impacted is education and schooling of children. However, this has also brought about the question of surveillance in schools and the consent of those who are being surveilled.

The United States has specific legislation for this - the Children's Online Privacy Protection Act ("**COPPA**"). If someone or something is collecting and sharing personal information about children under thirteen, it requires verifiable parental consent to be obtained. "Personal information" is defined as a child's name, address, phone number or email address, as well as any photos, videos, and audio recordings of the child and any persistent identifier such as IP address[92].

Australia does not have any legislation that is similar in nature to COPPA. Currently any privacy laws that relate to young people are covered by the Privacy Act. However, there are no provisions for children specifically, beyond the assumption that parents are responsible for making decisions for their children if they are unable to make the decision themselves[93]. Yet schools are using online surveillance technology to monitor children and their devices. These tools can track everything that the children are doing on the internet, and then report interactions they deem 'risky' or 'dangerous' to teachers and other school staff. This technology can be preloaded onto devices given to the students by the school, allowing this technology to monitor students outside of school hours[94]. Without the consent of the child or the parent, this is a large privacy breach, not to mention the problem with the collection and storage of data of those under the age of 18.

Suspect Targeted Management Plans (STMP)

The STMP is a police intelligence and risk assessment tool used by the New South Wales Police Force (NSW Police)[95]. It aims to prevent crime by targeting repeat offenders and possible future offenders. However there have been many issues with the use of STMPs, especially against young people and young indigenous people. Research findings by Sentas and Pandolfini found a disproportionate use of STMPs against young people and Aboriginal people[96]. There were even reported instances of use against children as young as ten which is below the age of criminal responsibility in that jurisdiction. STMP also encourages poor police practice, shows patterns of oppressive policing and increases young persons' contact with the criminal justice system with no impact on crime prevention. This pattern of oppressive policing and unfair targeting of Indigenous people can have a negative effect on their current and future offending. It marginalises young people and further stigmatises them from within their own communities[97].

This tool also has no transparency, no oversight, no scrutiny and no evaluation so it is unknown why people are placed on STMP or how they can be removed[98]. This shows the

[92] Federal Trade Commission. (2018) "Complying with COPPA." Retrieved from: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[93] Australian Law Reform Commission. (2018). "Existing Australian laws relating to privacy of individuals under the age of 18." Retrieved from: https://www.alrc.gov.au/publications/68.%20Decision%20Making%20by%20and%20for%20Individuals%20Under%20the%20Age%20of%2018/existing-australian-laws.

[94] Trevino, M. (2018). "Online Surveillance in schools: Student safeguard or privacy breach?" Melbourne: Education HQ Australia. Retrieved from: https://au.educationhq.com/news/49427/online-surveillance-in-schools-student-safeguard-or-privacy-breach/.

[95] Sentas, V., & Pandolfini, C. (2017). *Policing Young People in NSW: A Study of the Suspect Targeting Management Plan. A Report of the Youth Justice Coalition NSW*. Sydney: Youth Justice Coalition NSW. Retrieved from: http://www.yjc.org.au/resources/YJC-STMP-Report.pdf.

[96] Ibid.

[97] Ibid.

[98] Ibid.

unfortunate overlap in privacy issues between young people and Indigenous people, leading to a doubly significant negative impact on young Indigenous people.

Aboriginal and Torres Strait Islander People: Basics Card

A Basics Card is a form of welfare surveillance that mainly targets Indigenous Australians[99]. It was introduced in 2007 in the Northern Territory, under the Northern Territory Emergency Response ("**NTER**"). It is currently only implemented in the Northern Territory but there have been calls to roll this out in other states as well. The Basics Card sets aside a portion of someone's welfare entitlements, and places it on this card to be used only on pre-approved items[100]. These essential items include: food, clothing, food, rental payments and cleaning products. Restricted items include: alcohol, pornography, cash outs, vouchers and gift cards, cigarettes and cigarette products, gambling and brewing kits. These Basics Cards are forced income management, leading to feelings of stigma, untrustworthiness, lack of control and discrimination. There is also no means for current 'participants' to leave the scheme or have any means of redress[101].

In the context of data collection, sharing and profiling, the basics card also allows the Government to collect information on its users and catalogue what they spend their money on. This is targeted specifically at Indigenous people and the impacts are stronger due to their already marginalised and minority status.

Surveillance of Public Computers

As mentioned above, the government introduced the NTER in 2007 to try to reduce abuse and violence in remote Indigenous communities. One of the approaches is the surveillance of public funded computers and internet use. Between 2007 and 2012 the use of the computers and the records of the users were kept by the internet providers at the behest of the government[102]. By auditing the computers in the remote communities in NT, the government was surveilling an already marginalised and vulnerable group of people. Due to the digital inequality, the divide between technology availability in remote communities versus urban settings, allowed this kind of surveillance regime. Although the auditing was put in place to prevent exposure of pornography to women and children, it has a scope broader than its original purview. This can range from tracking computer use to criminal prosecution, from copyright infringement to breaches of privacy[103].

People with Low Socio-Economic Status: Facial Recognition use by Centrelink

Centrelink has said they will introduce facial recognition technology in order for welfare recipients to access the MyGov website and receive their Centrelink benefits[104]. This would link to the TDIF as mentioned above, created by the DTA. It would involve recipients uploading pictures of themselves to the government, which will then be checked against their driver's license or passport. These biosecurity measures are scheduled to start in October for the MyGov website and Centrelink next year.

[99] Dee, M. (2013). Welfare surveillance, income management and new paternalism in Australia. *Surveillance & Society* 11(3), 272-286.
[100] Ibid.
[101] Ibid.
[102] Rennie, E., Goldenfein, J., & Thomas, J. (2007). Internet policy and Australia's Northern Territory intervention. *Internet Policy Review,* 6(1), 1-17.
[103] Ibid.
[104] Lackey, B. (2018, July 2nd). Centrelink to face-scan welfare recipients in crackdown on fraud. *Daily Mail Online*. Retrieved from: http://www.dailymail.co.uk/news/article-5907569/Centrelink-face-scan-welfare-recipients-drastic-new-crackdown-benefits-fraud.html.

However, there are privacy issues with this kind of biometric data because once a database is created, there is the possibility of it being used by the government for other purposes. The other problem is being able to use someone else's photo to access their information through the online portal without their permission. Despite the difficulties of displaying a photograph to the sensor in public,[105] if imposters can bypass this challenge, it leaves Centrelink customers vulnerable to data breach.

Data discrimination: Targeting data collection towards minorities and vulnerable populations

There is growing recognition of the ways in which Australia's surveillance and data collection practices are targeted directly at, and significantly impact, minority and already marginalised populations, including Indigenous peoples, refugees and welfare recipients.[106] It is clear though scandals such as RoboDebt (as discussed above), regimes such as the BasicsCard,[107] Suspect Targeted Management Plans[108], the use of facial recognition by Centrelink,[109] and surveillance of public computers in remote Indigenous communities,[110] the Australian Government data practices assume somewhat of a colonial character. They are explicitly designed to target the most vulnerable and marginalised groups of our community. These groups already face challenges when attempting to fulfil their human rights due to a lack of power in society, so the addition of these targeted data collection initiatives only put further strain on these vulnerable populations. It is important that the Australian Government encourage, respect and promote Indigenous Data Sovereignty initiatives and associated principles and practices.[111]

Question 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?
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?
c) What principles should guide regulation in this area?

Gaps in Australian Law

This section canvasses some (but not all) of the main failings of Australia's human rights and privacy framework. It is worth noting at the outset that the *Privacy Act 1988* (Cth) is deficient compared to the new European GDPR. Further, Australia has failed to fulfil its obligations arising under the International Covenant on Civil and Political Rights. The systemic issues that we consider in this section include an absence of comprehensive constitutional protection of human rights, no cause of action for serious invasions of privacy (i.e. a privacy tort), narrow definitions of 'personal information' and significant exemptions to the *Privacy Act 1988* (Cth), and a captive and underfunded regulator.

These issues are compounded by a complete failure to meaningfully consult or consider the recommendations of civil society organisations.

[105] Smith, R. G. (2006). Identification systems: A risk assessment framework. *Trends and Issues in Crime and Criminal Justice, 324 (6),* 1-6. Retrieved from: https://gateway.library.qut.edu.au/login?url=https://search-proquest-com.ezp01.library.qut.edu.au/docview/189446979?accountid=13380
[106] Mann, M. & Daly, A. (2018). (Big) Data and the North-in-South: Informational Imperialism and Digital Colonialism in Australia. Special issue on Big Data from the South in *Television and New Media*, (forthcoming).
[107]Ibid.
[108]Ibid.
[109]Ibid.
[110]Ibid.
[111] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23). Canberra: Australian National University Press.

No constitutional protection of human rights

Currently in Australia there is no comprehensive constitutional protection of the general rights of citizens or a charter of human rights at the federal level,[112] which leaves citizens vulnerable to human rights infringements by both the state and other citizens.[113] In recent years Australian parliaments have demonstrated a willingness to pass laws that weaken the realisation of basic human rights such as freedom of speech and privacy.[114]

This is a significant gap in Australian law, leaving citizens vulnerable to human rights abuses, without the appropriate legislative protections.

Definitions of 'personal information' and exemptions from the Privacy Act 1988 (Cth)

The *Privacy Act 1988* (Cth) regulates the use and distribution of personal information. However, the law is limited by the definition of 'personal information'. As it defines 'personal information' as information that either includes identification of an individual or identifiable through data, it does not include peripheral data such as IP addresses, geolocation data or browsing history. Further, 'personal information' has been interpreted more narrowly than in Europe, and in Australia there is no indication of how to understand 'indirect' identification. Moreover, there are significant exemptions from the *Privacy Act 1988* (Cth). The Australian Law Reform Commission has criticised the number and scope of the exemptions.[115] For example, the *Privacy Act 1988* (Cth) does not apply to small businesses (annual turnover of less than AUS$3 million), media or political organisations.[116] There are also broad exemptions for enforcement agencies or agencies with enforcement functions. There is complete exemption for Australia's intelligence and security agencies.

No cause of action for serious invasions of privacy in Australia

The Australian law needs to catch up with current technological advances that impact on the human right to privacy (such as telephoto lenses, mobile phone cameras, the internet etc.). The Australian Law Reform Commission (ALRC) has called for enhanced privacy protections, in 2008[117] and more recently in its 2014 report, 'Serious Invasions of Privacy in the Digital Era'.[118] Australians have limited available legal avenues if their privacy is breached, the only means of complaint being through to the Privacy Commissioner. In Australia case law has followed the UK position that privacy is a species of confidence however breach of confidence has not proved itself to be as comprehensive a right as a clear right to privacy would afford.

[112] Kirby, M. (2009). *Arguments for an Australian Charter of Rights*. Ultimo, NSW: Constitutional Education Fund of Australia. Retrieved from: https://www.michaelkirby.com.au/images/stories/speeches/2000s/2009%2B/2398.Cefa_-_Blog_-_Arguments_For_Aust.Charter_Of_Rights.pdf.

[113] Williams, G. & Reynolds, D. (2017). *A charter of rights for Australia*. Sydney, NSW: NewSouth Publishing.

[114] Homer, R. (2017, August 10th). Time to fix Australia's odd absence of rights protections, *Financial Review*. Retrieved from: https://www.afr.com/business/legal/time-to-fix-australias-odd-absence-of-rights-protections-20170809-gxt0hh.

[115] Australian Law Reform Commission. (2008). Overview: Exemptions from the Privacy Act. In *For your information: Australian Privacy Law and Practice.* Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/publications/33.%20Overview%3A%20Exemptions%20from%20the%20Privacy%20Act/number-and-scope-exemptions

[116] Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era: Final report.* Canberra, ACT: Australian Government (p. 61, section 4.11). Retrieved from: https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf.

[117] Australian Law Reform Commission. (2008). *For your information: Australian Privacy Law and Practice Report*. Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/publications/report-108.

[118] Australian Law Reform Commission. (2014). *Serious invasions of privacy in the digital era: Final report.* Canberra, ACT: Australian Government. Retrieved from: https://www.alrc.gov.au/sites/default/files/pdfs/publications/final_report_123_whole_report.pdf.

Captive Regulator: Ineffective Federal Privacy Commissioner?

There has been a history of Government hostility towards the Office of the Australian Information Commissioner (OAIC) (and previous iterations of it). This has included, for example, attempts to abolish the office entirely,[119] as well as severe reductions in budgetary allocations. Both the role of Privacy Commissioner and the Information Commissioner are currently held by Angelene Falk, which was formally recognised on the 17th of August 2018. Angelene Falk has been in this position since the 24th of March 2018,[120] when the previous Privacy Commissioner Timothy Pilgrim retired.

In 2018, mandatory data breach notification legislation was introduced which is a welcomed development in the Australian privacy framework.[121] This requires eligible entities to report eligible data breaches to Federal Privacy Commissioner.[122] However, with the currently appointed Federal Privacy Commissioner only recently being appointed combined with the very limited funding to perform statutory functions, it is not clear how effective this scheme will be. Further, there are additional concerns as regards to the mandatory data breach notification scheme, such as a reactive rather than proactive approach to information security. The scheme is also limited in scope due to the focus on 'personal information' only, which may not take into account data collected by interconnected computing devices (Internet of Things (IoT)).[123] It also does not take into account breaches that affect commercially sensitive information or other data that is not considered 'personal' as per the criticism of the narrow definition of personal information as discussed above.[124]

Successive Privacy Commissioners have also failed to make section 52 determinations and plaintiffs or defendants are unable to compel them to do so. Between 1988 and 2015 only ten determinations awarding compensation were made under Section 52 of the *Australian Privacy Act 1988* (Cth).[125] These are when the Commissioner can either dismiss a complaint after an investigation or they can find that a complaint has merit. Should the complaint be substantiated they can declare that the respondent must; a) take specific steps with a specific time period to stop and not repeat the particular conduct; b) perform an act or series of acts to redress loss and damages; c) compensate the complainant monetarily for any loss or damage; or d) decide to take no further action.[126]

It is essential that people have a clear path to access justice when they have been the victim of a privacy breach. The OAIC dispute resolution mechanism is currently deficient as it does not meet the standards of other dispute resolution processes (such as the current Financial Ombudsman Service). There is also a fundamental conflict of interest with a regulator also running a dispute resolution process. With a continuing reduction in government funding for the OAIC, it is necessary to consider a "user pays" system where organisations regulated by the *Privacy Act 1988* are required to pay for dispute resolution matters to be resolved (in the same way financial services providers pay for dispute resolution).[127]

[119] *Freedom of Information Amendment (New Arrangements) Bill 2014* (Cth) (Austl.)

[120] Office of the Australian Information Commissioner. (2018, March 23rd). *Farewell to Timothy Pilgrim PSM - Australian Information Commissioner and Australian Privacy Commissioner*. Canberra, ACT: Australian Government. Retrieved from: https://www.oaic.gov.au/media-and-speeches/news/farewell-to-timothy-pilgrim-psm-australian-information-commissioner-and-australian-privacy-commissioner.

[121] Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view, Computer Law & Security Review: *The International Journal of Technology Law and Practice*, 34(3), 477-495.

[122] Australian Institute of Criminology. (n.d.) *Notifiable data breaches scheme*. Canberra: Australian Government. Retrieved from: https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme.

[123] Daly, A. (2018). The introduction of data breach notification legislation in Australia: A comparative view, *Computer Law & Security Review: The International Journal of Technology Law and Practice, 34*(3), 477-495.

[124] Ibid.

[125] Gunning, P. (2015, April 29th). Another privacy commissioner determination awarding compensation, *IP Whiteboard.* Retrieved from: http://ipwhiteboard.com.au/another-privacy-commissioner-determination-awarding-compensation/.

[126] Federal Register of Legislation. *Privacy Act 1988.* Retrieved from: https://www.legislation.gov.au/Details/C2018C00292.

[127] It is noted that AFCA currently handles Privacy Act disputes relating to credit reporting.

Question 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?

Industry self-regulation has historically been less than successful in resolving privacy problems on its own. Towards the end of the .com bubble, researchers were already noting the lack of an effective industry self-regulatory regime for dealing with online consumer privacy issues. If anything, industry self-regulation has only made the situation worse for privacy issues, creating a more permissive environment for the collection and use of individuals information.

The APF Policy Principles on Privacy:

The APF is the primary association dedicated to protecting the privacy rights of Australians. The APF aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. Although the APF Policy Principles are not technologically specific they do apply in relation to new and emerging technologies[128].

The APF strongly suggests that the human rights expressed in International Covenant on Civil and Political Rights (ICCPR) be entrenched in the Australian Constitution, in a form that ensures that they are enforceable. However, the APF understands that achieving constitutional reform can be difficult, so recommends some interim measures. The privacy areas that should be included in these interim measures are: privacy of the physical person, privacy of personal behaviour, privacy of personal communications, privacy of personal data and privacy of personal experience. The APF also suggests that all Australian Parliaments need to enact legislation that ensures that all human rights expressed in ICCPR are implemented, and in such a manner that the rights are comprehensive, non-discriminatory, enforceable, and enforced.

The APF and the QCCL commends the Queensland government's commitment to enact a Human Rights Act, and supports the efforts in Tasmania to get a Bill of Rights onto the political agenda.

Additional Approaches to Human Rights Protection: Data Protection by Design and by Default

Privacy and data protection should be designed within systems and built in by default rather than be a reactive or remedial design after a breach. By design and by default aim to prevent breaches and actively stop them from occurring rather than merely trying to fix the problem after it happens. It makes privacy the default option, even if the end user does not do anything, all of their information should be protected by the system automatically. Privacy and data protection should be fully built into the system, with full functionality without affecting the running of the system.

One way to facilitate the broader adoption of privacy-by-design principles would involve a sustained program in human rights education for technology professionals. For example, the programmers who are responsible for the design and development of these technical systems, and of the algorithms behind all of these systems, do not typically receive training

[128] Australian Privacy Foundation. (2018). Human Rights Protections. Retrieved from: https://privacy.org.au/policies/human-rights/.

in human rights law[129] or are otherwise not financially motivated to ensure that the system is focused on privacy.

These software engineers are in effect interpreting, applying and potentially even breaching human rights law.[130] Improved understandings of human rights and human rights law could help technology professionals understand issues such as indirect discrimination, is and why it is prohibited by law. In particular, better understanding of the right to a fair trial and the presumption of innocence could lead to improved design for algorithms, to prevent the introduction of discriminatory biases.[131]

It is also important to ensure that algorithms used in the provision of justice are made open to ensure that transparent and fair process are applied to the Court's interpretation and application of new technologies.

"Mates don't let mates drink and selfie" - Social Marketing approaches to Privacy

At the heart of new discussions and negotiations about privacy is a role for social marketing practice in facilitating and effecting change through further research about consumer and industry behaviours; and the planning of strategies that target actors at all levels of the market system. On an individual level, there is a need for persuasive messages to motivate people to more actively engage with privacy issues, transforming them from passive individual targets of privacy invasion to agents of privacy advocacy within their social groups. Industry must also be persuaded to look beyond short-term profits from exploiting personal information, to a socially and commercially sustainable approach to consumer data. To demonstrate good corporate citizenship, firms must go beyond just legal responsibilities, and consider their broader ethical responsibilities to society. Persuading both groups to engage with privacy issues, and to collaborate on finding workable solutions, will be needed if improvements are to be made in addressing the current problems confronting privacy issues in today's markets.

Some current early strategies include: persuading industry to adopt consumer privacy issues as a matter of corporate social responsibility; encouraging improved industry self-regulation, such as requiring greater transparency and clarity in privacy policies, particularly in relation to the changes in these policies over time; and promoting a move (back) towards business models where consumers (and their data) are treated as customers rather than products to be sold to advertisers. While shifts away from the current business model would potentially have significant impacts on a broad range of stakeholders, specifically advertisers, the protection of profits cannot be put above the protection of the fundamental right to privacy.

Question 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?

Applications of AI that Threaten Human Rights: Use of AI in the Canadian Immigration and Refugee System

Since 2014, the Canadian immigration and refugee system has been testing algorithms and other AI technology to replace or augment administrative decision-making.[132] These

[129] Beduschi, A. (2018, September 26). Technology dominates our lives – that's why we should teach human rights law to software engineers. *The Conversation.* Retrieved from: https://theconversation.com/technology-dominates-our-lives-thats-why-we-should-teach-human-rights-law-to-software-engineers-102530.
[130] Ibid.
[131] Ibid.
[132] Macnab, A. (2018, September 26). Report says use of AI could be violating human rights. *Canadian Lawyer.* Retrieved from: https://www.canadianlawyermag.com/legalfeeds/author/aidan-macnab/report-says-use-of-ai-could-be-violating-human-rights-

automated decision-making systems have been operating without independent oversight.[133] Algorithms are designed to identify merits of an immigration application, spot potential red flags and consider all of these factors and provide a recommendation as to whether the applicant should be accepted.[134] This application of AI decision-making emerged in response to extensive backlogs and delays within the immigration system.[135]

Although the system remains in the development stages, there is some form of automated system being used to "triage" applications into two streams; "simple" cases are processed by the algorithm and "complex" cases are flagged for review.[136] As the immigration and refugee system deals with vulnerable groups such as non-citizens, and people from linguistically diverse backgrounds, the use of AI decision-making and predictive analysis raises concerns surrounding the impact upon human rights for these vulnerable and under-resourced communities.[137]

Correctional Offender Management Profiling for Alternative Sanctions (COMPAS)

COMPAS is a pre-crime algorithm that predicts a defendant's risk of recidivism by considering answers from a 137-item questionnaire.[138] Offenders are each given a score from 1 to 10, with higher scores meaning greater risk.[139] This automated decision-making algorithm is used to decide the fate of offenders throughout the justice system.[140] Despite the opportunity for this algorithm to potentially streamline the criminal justice system and reduce the incarceration of offenders who pose no threat to society, it was found that COMPAS is no better at predicting an individual's risk of reoffending than random volunteers recruited from the internet.[141] In addition to its inaccuracies, the algorithm was also found to be biased against African Americans, with people of colour being almost twice as likely as white people to be labelled "high risk" but not actually go on and reoffend.[142] The opposite mistake was made in cases with white offenders, as the algorithm had labelled white offenders who went on to commit further crimes as "low-risk". [143]

As COMPAS is proprietary system, the criteria used by the algorithm is secret and offenders are not able to access their results.[144] This raises concerns as to the validity of the results, as it is known that data f[145]rom the criminal justice system is often unreliable. Defendants should be able to review the algorithm and challenge the validity of the report within the court, and by denying them the opportunity to do so is the trial really fair?[146] The use of

16279/. ; Molnar, P, and Gill, L. (2018). Bots at the gate: A human rights analysis of automated decision making in Canada's immigration and refugee system. *The Citizen Lab.* Retrieved from: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

[133] Macnab, A. (2018, September 26). Report says use of AI could be violating human rights. *Canadian Lawyer.* Retrieved from: https://www.canadianlawyermag.com/legalfeeds/author/aidan-macnab/report-says-use-of-ai-could-be-violating-human-rights-16279/.

[134] Ibid.

[135] Ibid.

[136] Ibid.

[137] Molnar, P, and Gill, L. (2018). Bots at the gate: A human rights analysis of automated decision making in Canada's immigration and refugee system. *The Citizen Lab.* Retrieved from: https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.

[138] Yong, E. (2018, January 17). A Popular Algorithm Is No Better at Predicting Crimes Than Random People. *The Atlantic.* Retrieved from: https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/.

[139] Verbruggen, R. (2016, August 2). Does Pre-Crime Have a Race Problem?. *The American Conservative*. Retrieved from: https://www.theamericanconservative.com/articles/does-pre-crime-have-a-race-problem/.

[140] Ibid.

[141] Yong, E. (2018, January 17). A Popular Algorithm Is No Better at Predicting Crimes Than Random People. *The Atlantic.* Retrieved from: https://www.theatlantic.com/technology/archive/2018/01/equivant-compas-algorithm/550646/.

[142] Ibid.

[143] Ibid.

[144] Smith, M. (2016, June 22). In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. *The New York Times.* Retrieved from: https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?_r=0.

[145] Ibid.

[146] Ibid.

COMPAS to inform sentencing also denies offends the right to have an individualised sentence, which further accentuates the inequalities present within the criminal justice system.

Applications of AI that Protect Human Rights: Automatic Exploit Generation (AEG)

AEG is the first end-to-end system of fully automatic exploit generation that finds bugs automatically and determines if they are exploitable.[147] If bugs are found, the AEG secures the vulnerabilities and produces an intrusion detection system signature that will recognise future exploits and exploit variants.[148] This software defends data against both human hackers and intelligent computer viruses, providing protection from the individual level to a national level, preventing data misuse and unauthorised access.[149] Although this tool is very useful in providing a defence against data misuse, there is a need to progress security initiatives further so they can perform prescriptive analytics.

PatternEx AI^2

Upon recognising the extreme data vulnerabilities facing modern enterprises, PatternEx developed a new cybersecurity AI program that they claim solves the issues that plague simple machine learning.[150] AI^2 is designed to detect malicious user intent by observing user behaviour and applying AI models, and once malicious intent is confirmed, the program takes action automatically to challenge, delay or block the user.[151] The program continuously incorporates input from human experts to provide more accurate predictions of cyber attacks.[152] It is reported that AI^2 had increased attack detection rate by a factor of 10, and decreased false positive rate by a factor of five when compared to machine learning-only solutions.[153] This continuous loop of feedback between the human analyst and AI system allows the system to learn in real-time, and be adaptive to new threats posed by cyber-criminals, as the human analysts provide feedback to the system which further sharpens the systems precision.[154] The application of AI^2 provides organisations with the opportunity to protect their users/customers data is a proactive manner, that seeks to predict attacks before they happen and prevent them. AI^2 is an example of an AI program that strengthens the privacy of all consumers data and provides a technique of protection that is constantly evolving to face new threats posed by cyber criminals.

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

As discussed in this submission, there is significant scope of abuse when AI-informed decision-making is being used without adequate supervision or is otherwise cloaked in intellectual property (including trade secret protection).

We respectfully submit that Australian law ought to recognise the powerful *assumptions* that AI can make based on big data and complex variables; however, we submit that reliance

[147] Faggella, D. (2017, September 17). Artificial Intelligence and Security: Current Applications and Tomorrow's Potentials. *TechEmergence.* Retrieved from: https://www.techemergence.com/artificial-intelligence-and-security-applications/.
[148]Avgerinos, T. Cha, S. Hao, B. & Brumley, D. (2014). Automated exploit generation. *Communications of the ACM, 57 (2),* 74-84. DOI: 10.1145/2560217.2560219.
[149] Faggella, D. (2017, September 17). Artificial Intelligence and Security: Current Applications and Tomorrow's Potentials. *TechEmergence.* Retrieved from: https://www.techemergence.com/artificial-intelligence-and-security-applications/.
[150] PatternEx. (2016). *Redefining InfoSec By Combining AI and Human Intuition*. Retrieved from: https://www.patternex.com/architecture-patternex-virtual-analyst-platform-wp?hsCtaTracking=41b5ae10-d518-4aee-80ec-1194a6bc6463%7C432c1363-8059-4675-a780-8ea1da8a93e9.
[151] Ibid.
[152] Ibid.
[153] Ibid.
[154] Ibid.

upon AI ought only to occur when the underlying algorithms and, data correlations, assumptions and degrees of certainty are publicly (and actively made) available.

New York City - Automated Decision Systems Task Force

In New York City, an Automated Decision Systems Task Force ("**ADS Task Force**") has been created to provide recommendations regarding a process for reviewing the government's use of algorithms to make automated decisions.[155] The ADS Tas Force aim's to ensure decisions made by algorithms within New York City align with the goal of creating a fairer and more equitable city.[156] Representatives from government agencies, non-profit, and academia will all collaborate to provide recommendations by early 2019.[157] The final report will identify which city agencies need reviewing, recommend procedures for requesting explanations of algorithmic decisions, and explore a procedure which the city can use to determine if an automated decision disproportionately impacts persons based on factors such as age, race, religion or sexual orientation.[158]

The first draft of the bill including extensive reporting requirements, compelling agencies to provide the task force with relevant information, the draft was rejected by city administration.[159] The ADS Task Force now has only voluntary disclosures to rely on, granting the government body no real legal powers, and raising many concerns as to the quality of the report the task force will be able to produce.[160]

Question 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?

Following the Senate inquiry into Centrelink's data matching program, algorithmic decision-making has become a high-profile issue in Australia. This is also an emerging issue in many countries, with new regulations being proposed. While provisions for computerised decision-making exist in various Australian laws, their impacts are poorly understood. Algorithmic decision-making has the potential to improve the efficiency and accuracy of government decision-making but can also be used in ways that are harmful to individuals.[161] This may include pre-existing biases being built into algorithms that target 'risky' individuals or already marginalised groups.[162]

[155] City of New York. (2018). ADS Taskforce. *New York City Mayor's Officer of Operations.* Retrieved from: https://www1.nyc.gov/site/operations/projects/ads-task-force.page.
[156] Ibid.
[157] Ibid.
[158] Stiefel, M. (2018, July 31). New York Creates Task Force to Examine Automated Decision Making. *InfoQ*. Retrieved from: https://www.infoq.com/news/2018/07/NYC-taskforce-automated-decision.
[159] Powels, J. (2017, December 20). New York City's Bold, Flawed Attempt to Make Algorithms Accountable. *The New Yorker.* Retrieved from: https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable.
[160] Ibid.
[161] Bennett-Moses, L. & Chan, J. (2014). Using big data for legal and law enforcement decisions: Testing the new tools. UNSW Law Journal. 37(2), 643-678.
[162] Friedman, B. & Nissenbaum, H. (1996). Bias in computer systems. ACM Transactions on Information Systems, 14(3), 330-347.; Lum, K. & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14-19.; Eubanks, V. (2018). *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor.* First Edition., New York, NY: St. Martin's Press.; Mann, M. & Daly, A. (forthcoming). (Big) Data and the North-in-South: Australia's Informational Imperialism and Digital Colonialism. *Television and New Media special issue on 'Big Data from the South'*, edited by Stefania Milan and Emiliano Trere. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248936.

The use of algorithms in criminal justice contexts has the potential to be particularly problematic as it can involve targeting surveillance and policing activities, or increased monitoring of those released from prison on the basis of predicted risk. Algorithmic justice attempts to make decision-making more 'efficient' and 'objective' through actuarial assessment.[163] However, these processes are not neutral, and bias becomes inscrutable and incontestable with increased barriers to transparency via a potentially false veil of objectivity provided by computerisation (Friedman & Nissenbaum, 1996).

Dataset validity and the impacts of error were also identified in the recent Australian Senate Community Affairs References Committee inquiry (2017) into the Centrelink automated data-matching program that sought to identify discrepancies in income reporting and automatically suspend social security payments.

In striving for increased efficiency through automation, procedural and due process safeguards may be undercut. This is because divisions between surveillance, adjudication and punishment are eroding with new forms of surveillance and automated decision-making that remove humans entirely having the potential to collapse these processes (Marks et al., 2017).

There is recognition of both the importance of, and difficulties in, developing accountability structures for algorithms.[164] There have been some attempts to regulate algorithms through the new GDPR. Aspects of the GDPR explicitly relate to algorithmic profiling, automated decisions making, and a so called 'right to explanation for automated decision-making'. It has been argued that the GDPR could "require a complete overhaul of standard and widely used algorithmic techniques" but the exact impacts on computerised decision-making are yet to be resolved[165].

Relevant areas of law include human rights, data protection, anti-discrimination law and areas of intellectual property law. Trade secrecy and other intellectual property rights may mean algorithmic decision-making is not legally challengeable (exemplified by the COMPAS algorithm[166]). These fields of law become crucial for offering new avenues to hold algorithmic decision-making to account.

Question 8: What opportunities and challenges currently exist for people with disability accessing technology?

As expressed in the introduction to this submission, technology is a tool that can be used both for benevolent and malevolent purposes. We respectfully repeat the submissions made in response to the foregoing questions in response to this question.

There is significant scope for persons with disability to benefit from technology that currently exists and will continue to be developed.

It is our submission that the challenge is that any technology can be repurposed in the future and therefore safeguards must be put into place as soon as practicably possible to ensure

[163] Harcourt, B. (2005). "Against prediction: Sentencing, policing, and punishing in an actuarial age." *University of Chicago Public Law & Legal Theory Working Paper*, No. 94.

[164] Bennett-Moses, L. & Chan, J. (2016). Algorithmic prediction in policing: Assumptions, evaluation and accountability, Policing and Society, online first.; Vedder, A. & Naudts, L. (2017). "Accountability for the use of algorithms in a big data environment." *International Review of Law, Computers & and Technology*.

[165] See: Goodman & Plaxman, 2016, p. 26. Retrieved from: https://www.researchgate.net/publication/304548505_EU_regulations_on_algorithmic_decision-making_and_a_right_to_explanation.

[166] Smith, M. (2016, June 22). In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. *The New York Times.* Retrieved from: https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html?_r=0.

that technology is consumed on an informed basis and that avenues of recourse exist to ensure that checks and balances are constantly able to be applied to the development, application and use of technology.

Question 9: What should be the Australian Government's strategy in promoting accessible technology for people with disability

We submit that a strategy to promote accessible technology must start with an enforceable federal human rights framework that serves as the basis of a check and balance to the misuse of technology. This ought to be coupled with the principles of "privacy by design" and informed consent with the rights to explanation and transparency in the manner in which data is used, particular in AI-informed decision making.

We submit that this would be best matched with a comprehensive overhaul of school education, university education and workplace education to include a comprehensive agenda for human rights. We consider that this is of paramount in ensuring that *all* Australians, including those with disability, understand their human rights (as they exist in international law), the consequences of the consumption of technology and the (currently minimal) recourse and remedies that they have in relation to their human rights.

We recommend that the Commission review the scope, manner and extent of human rights education at all levels in Australia.

Question 10: How can the private sector be encouraged or incentivised to develop and use accessible and inclusive technology, for example, through the use of universal design?

We respectfully repeat and reiterate the submissions made to previous Issues Paper questions and further submit that the private sector ought to be encouraged by clear and enforceable federal human rights legislative framework that incorporates privacy as a complex and interwoven rights that underpins human dignity.

It is also relevant to note that a complex interaction exists between the need for information to be freely accessible and available and the consequence of monopoly-based intellectual property regimes[167].

It is our submission that a combination of market-based incentives such as human rights compliant certification, the architectural principles of privacy by design, a reconsideration of how intellectual property operates[168] in the context of a globalised and digitalised world together with a socially focused education would encourage the development of accessible and inclusive technology and alleviate intellectual property issues with universal design.

Conclusion

We thank the Commissioner for the opportunity to provide this submission and we reiterate that technology is not good or bad – it is merely a tool. We have provided some short examples of positive applications of technology which benefit human rights; however, we have outlined a position which demonstrates that technology can also be used malevolently

[167] See for example: Murray, A., (2014). *Copyright Enforcement for Internet Based Material Infringements and the Personal Right of Privacy: A Comparative Study Between Australia and the European Union Member States, with a Focus on the United Kingdom*. Nordiskt Immateriellt Rättsskydd. Retrieved from: http://www.nir.nu/Journal/953/nir-2014-1.

[168] See for example: Giblin, R., & Weatherall, K. (Eds.). (2017). *What if we could reimagine copyright?* Acton: ANU Press. Retrieved from http://www.jstor.org/stable/j.ctt1q1crjg.

and technology that was created with the best intentions can be manipulated and used to oppress.

It is our submission that a large number of the concerns contained in this submission *may* be able to be alleviated with an increased focused on human rights education and the introduction of a comprehensive and enforceable federal Human Rights legislative framework.

We look forward to continuing consultation on this important issue and have provided key recommendations for the Australian Human Rights Commission to consider in advancing the protection of privacy and other human rights in response to new and emerging technological developments.

Recommendations

We suggest that the following recommendations are important areas of reform and go some of the way to addressing the systemic issues as described above:

1. Introduce an enforceable charter or bill of human rights at the federal level;

2. Introduce a privacy tort or cause of action for serious invasions of privacy;

3. Improve and increase Australian human rights education at all levels, including schools and workplaces;

4. Release clear and considered guidelines for the development, implementation, application and review of automated decision-making technology with a view to incorporating such provisions into the *Privacy Act 1988* or legislation analogous to the GDPR;

5. Undertake a similar process to the European Parliament's Report with recommendations to the European Commission on civil law rules on Robotics[169];

6. Introduce a Biometrics Commissioner;
7. Amend the definition of "personal information" to expressly acknowledge that metadata is capable of being used to identify an individual;

8. Review the Privacy Act 1988 to ensure it meets international best practice on privacy.

9. Increase funding to the Office of the Australian Information Commission to enable them to undertake their statutory functions;

10. Improve access to justice for privacy disputes by requiring all organisations regulated by the Privacy Act 1988 to provide access to a free external dispute resolution scheme.

11. Propose ethical technologic creation (including assurances that technology is not built with intentional security weaknesses) and destruction guidelines which incorporate human rights protections;

12. Implement principles of privacy-by-design and data-protection-by-design and default;

[169] See: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//EN.

13. Recognise that a loss of privacy (as a fundamental and foundational right) has further impacts, for example, the discriminatory impacts of data collection and use targeted towards vulnerable groups and the information security impacts of weakening encrypted form of communication;

14. Acknowledge that the development, creation and disposal of technology has an international environmental and social consequence;

15. Review the scope, manner and extent of human rights education at all levels in Australia; and

16. Encourage and promote Indigenous Data Sovereignty initiatives and associated principles in the collection and use of information concerning Australia's Indigenous Peoples.[170]

[170] See for example: Kukutai, T., & Taylor, J. (2016). Data Sovereignty for indigenous peoples: current practice and future needs. In *Indigenous Data Sovereignty: Towards an Agenda* (1-23), Canberra: Australian National University Press.

About Us

Australian Privacy Foundation

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians.

See more: https://privacy.org.au/

The Queensland Council for Civil Liberties

The Queensland Council for Civil Liberties (QCCL) is a voluntary organisation concerned with the protection of individual rights and civil liberties. It was founded in 1966 in order to protect and promote the human rights and freedoms of Queensland citizens. Since then the QCCL has worked ceaselessly to promote civil liberties. QCCL works towards a society in which the human rights enshrined in such documents as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, to which Australia is signatory, are enjoyed by all Queenslanders and indeed Australian citizens.

See more: https://qccl.org.au/

Electronic Frontiers Australia

Electronic Frontiers Australia Inc. is a non-profit national organisation that has been promoting and protecting digital rights (civil liberties) in Australia since it was established in January 1994. EFA serves to protect and promote the civil liberties of users of computer-based communications systems and of those affected by their use.

See more: https://www.efa.org.au/