STATE OF DIGITAL RIGHTS

MAY 2018

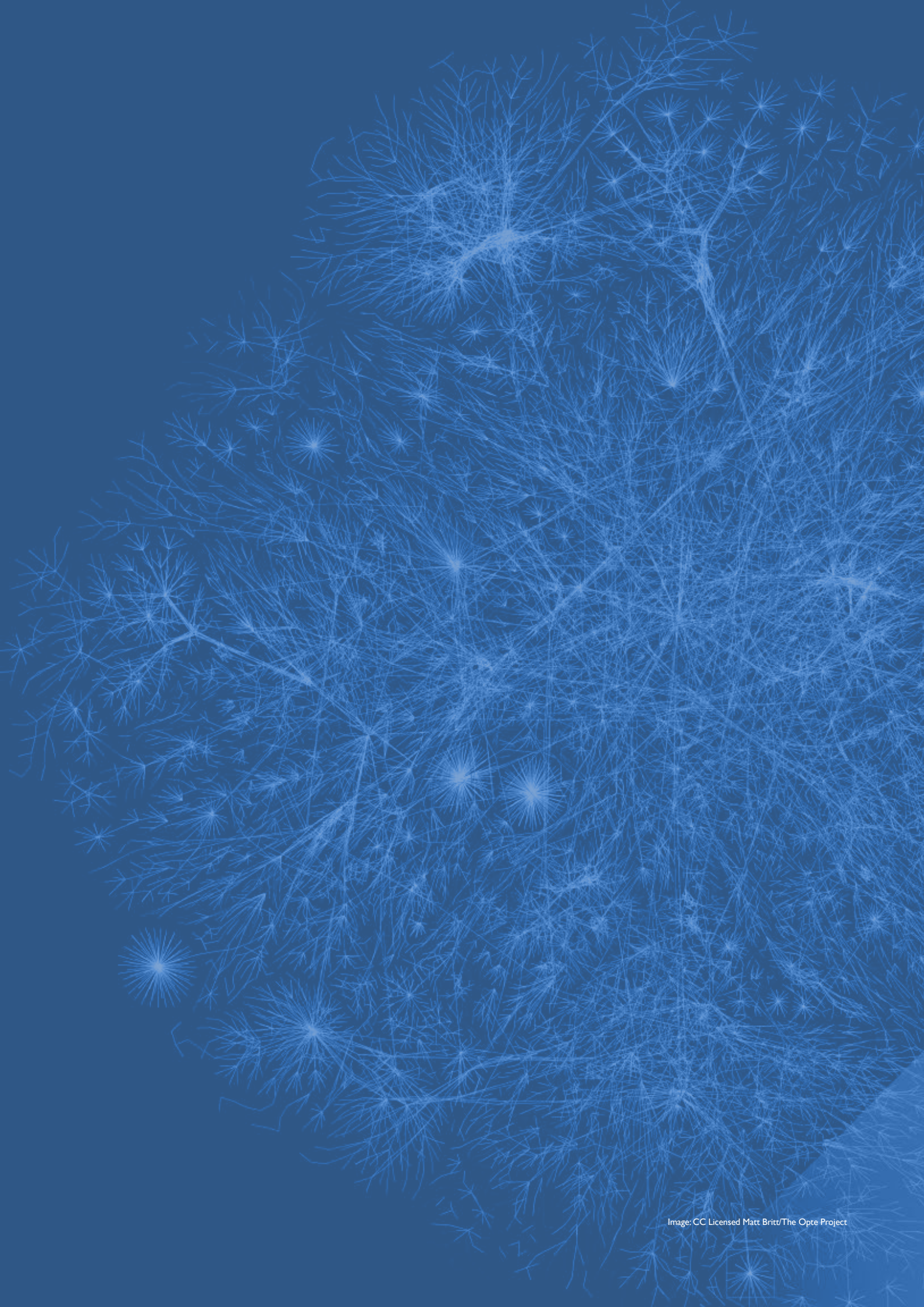


Image: CC Licensed Matt Britt/The Opte Project

CONTENTS

Foreword - Professor Gillian Triggs

The central message of this report is that the impact of digital regulation should be viewed through the prism of human rights law.

Government attempts to control the digital world pose an inevitable tension between two fundamental human rights: fair access to the internet and personal rights to privacy and freedom of expression.

I know from my own experience as the President of the Australian Human Rights Commission that there are very real concerns around the protection of individual rights against the unprecedented avalanche of laws passed by federal Parliament to counter terrorism. Indeed, the 9/11 attacks on the United States have been a catalyst, or camouflage, for the enactment of a vast body of national security laws. About 70 separate pieces of legislation have been introduced since 2001, including mandatory data retention, mass surveillance and intelligence sharing.

It is timely that we should assess the validity of new laws regulating data by benchmarking them against Australia's human rights obligations, particularly under the International Covenant on Civil and Political Rights. Are such laws, for example, a threat to democracy by chipping away at our common law freedoms of speech and association and the right to privacy?

In 2015, the Government passed changes to the Telecommunications (Interception and Access) Act that compel telecommunications providers to retain metadata collected from their users for at least two years. No warrant or judicial supervision is required for ASIO and other government agents to have access to the metadata retained in this way. Since the mandatory data retention laws were passed, about 60 agencies have asked for access to the data. Traditional law requires that the content of an email or phone call may be accessed only with a prior judicial warrant. Ironically, access to metadata without a warrant, will reveal more about a person and their network of relationships than will the content of an email or phone call.

Exceptionally, a warrant will be necessary for access to metadata if a security agency wants to access a journalist's data, presumably to protect sources. It is hard to understand why the rest of the Australian community is subject to metadata retention laws without a warrant to justify the significant loss of privacy. In addition to concerns about privacy is the chilling effect that metadata retention laws are likely to have on freedom of speech and association.

I have a personal experience of the dangers of data retention laws. In August 2017, I was asked by Digital Rights Watch to contribute to a Melbourne Writers Festival panel on digital rights. I agreed to provide 24 hours of my digital life; to whom I had sent emails and texts; where I travelled in Melbourne and all phone calls made to and from me. My life is an open book. What could possibly go wrong? As I sat before the audience, details of my pristine life were thrown up on the screen behind me. I heard titters from the audience and realised that something

was amusing. It seems that one of my emails was an application for a Seniors Card! Such unfiltered access to our personal data reveals far more than we might imagine.

One of my functions as president of the Human Rights Commission was to monitor conditions for those detained, often for years, in immigration facilities on Christmas Island and mainland centres. One of the concerns of detainees is that their conditions depend on whether they are assessed as high, medium or law security risks. Determination of the level of risk seemed to detainees to be arbitrary. I asked the Superintendent how risk levels are assessed. He replied that they are 'based on an algorithm'. When I looked rather shocked, he added that the algorithm will be moderated by his personal assessment. I accept that he genuinely tried to make a fair judgment. The problem remains that an algorithm informs most risk assessments, and adds to the sense of disempowerment of a detainee who is held without charge or trial at the discretion of the Minister.

During a radio interview, I expressed my concerns about the use of algorithms, attracting some strong contrary views. One young man, an IT expert and social justice advocate, told me that an algorithm would avoid the risks of subjective and biased judgments and be more consistent. Perhaps he is right. To trust in the presence of an empathetic and fair-minded superintendent is risky. Nonetheless, I remain to be convinced, preferring a humane personal judgment behind any decision to deny fundamental rights.

Another troubling aspect of data collection is the potential for breaches. In 2014, for example, the Department of Immigration accidentally released the personal data relating to 10,000 asylum seekers. As many asylum seekers may be deported to their country of nationality, there is a risk that they will be persecuted, arrested and tortured. The legal costs for the Department are estimated to be over $1 million by 2017, with 34 matters related to the breach before the Federal Circuit Court, six in the Federal Court and one in the High Court.

While accurate figures are impossible to obtain, the Minister for Law Enforcement and Cyber Security, estimated that in 2017 there were 734 cyber incidents in private sector systems affecting the national interest. In early 2018, the Government introduced laws requiring companies to report to the Information Commissioner any data breaches that have potentially harmful effects. Overwhelmingly, the personal identifiable information that is susceptible to identity theft relates to credit and debit card information, names and bank account details. While Australia's reporting laws come 16 years after the introduction of similar laws in the United States, they are designed to strengthen cyber security and, in turn, to improve confidence in business and government.

I commend *The State of Digital Rights Report (2018)* in drawing attention to the human rights impacts of the digital age.

Professor Gillian Triggs

Introduction

In the space of just a few years, the human rights movement has crashed into a technological, social and moral wall. The true impacts of serious violations of our personal digital rights are starting to hit very close to home for a lot of people, and the world will never be the same.

The revelations put forward by Edward Snowden on the scale and reach of the United States' surveillance capability, whistleblowing by Chelsea Manning that blew the lid off military manipulation, corruption and coercion, the exposure of mass-manipulation of democratic elections by Cambridge Analytica - all of these have certainly contributed to a heightened awareness of the potential impact of digital rights. But these high-profile incidents are just scratching the surface of a much wider, systematic and willful degradation of our human rights online.

The internet is often touted as the new frontier of freedom of expression, described simultaneously as a wide open plain free from heavy-handed intervention - or a lawless landscape that political leaders struggle to understand and fail to police. The pervasive rise of personal digital technology offers the potential to realise many human rights. Vast amounts of our lives now take place online, including paid employment, participating in democracy and communicating with government and with each other.

This can be liberating: it is possible to engage with the internet anonymously, to communicate secretly and access services and communities that allow us to be ourselves, without fear of judgement. But there is also a dark side to life in the digital age that includes surveillance of populations, tracking of individual movements or conversations and data-matching on a global scale. It's clear that corporate and government power over our digital lives need to be kept in check.

Digital rights are inherent human rights. And just as other human rights are far from inalienable, digital rights must be fought for, solidified into social normality and ultimately protected and upheld if we are to maintain our humanity in digital spaces.

Every public space is subject to regulation, just like every human right involves some form of balancing with other rights. How do we make the most of what digital life offers, allowing the free and open exchange of ideas, whilst also ensure that adequate protections are put in place? An unregulated internet is not the same as a free and open one. To create inclusiveness online, and create accountability for abuse and harassment, we need rules of conduct and designers who are sensitive to the experience of vulnerable people.

Upholding digital rights requires us to find the balance between the opportunity the internet provides us to live better, brighter and more interconnected lives, and the threat, posed by trolls, corporations and government. Ideally it will involve law making that includes educated community participation and generates nuanced public debate.

This report aims to support, enhance and promote that debate, through analysing a select few of the key digital rights issues facing Australians today, and making clear recommendations for policy makers to adopt. A critical step towards upholding our human rights in a technological age is to understand that digital rights are human rights that are expressed online. We must protect these rights, whatever the cost.

Tim Singleton Norton - Chair, Digital Rights Watch

Photo: CC Licensed Andrew Malone

Recommendations

Repealing metadata retention

- The Australian Government should immediately repeal the metadata retention regime or introduce significant amendments to existing legislation to put in place proper safeguards consistent with the rights to privacy and freedom of expression.

Protecting privacy

- The Australian Government should introduce legislation that respects and upholds the right to digital privacy and to data protection.
- Investigate the creation of a similar body to the European Data Protection Authorities and task this body with upholding and monitory privacy protections, including digital rights in the workplace.
- Explore the possibility of a 'right to disconnect' that would regulate employer's use of digital tools to make sure that this does not encroach on statutory periods of rest and holidays of employees.
- Privacy, data protection, anti-discrimination, right to explanation, and review and appeal regulatory structures and policy frameworks should be considered in localised contexts, prior to implementation of big data policing and algorithmic profiling.
- Implement the 2014 Australian Law Reform Commission recommendations for the introduction of a Commonwealth statutory civil cause of action for serious invasions of privacy, including digital privacy.
- Expand the definition of sensitive information under the Privacy Act to specifically include behavioural biometrics.
- Increase measures to educate private businesses and other entities of their responsibilities under the Privacy Act regarding behavioural biometrics, and the right to pseudonymity.
- Investigate the development of a free and easily accessible national data and movement-tracking opt-out register for people who do not want their sensitive data to be collected for commercial uses.
- Introduce a compulsory register of entities that collect static and behavioural biometric data, to provide the public with information about the entities that are collecting biometric data and for what purpose.

Intelligence sharing operations

- The loopholes opened with the 2011 reform of the FOI laws should be closed by returning ASD, ASIO, ASIS and other intelligence agencies to the ambit of the FOI Act, with the interpretation of national security as a ground for refusal of FOI requests being reviewed and narrowed.
- A new agreement negotiated among the Five Eyes governments that any information held by the United States on nationals of the other countries be stored only within the borders of that country and unless directly related to a national security operation or criminal trial, be accessible only with the approval of the home government, with an annual report of how many requests for access have been made.
- A complete cessation of commercial espionage conducted by the Australian Signals Directorate.
- Expansion of powers of the Joint Parliamentary Committee on Intelligence and Security to initiate its own reviews into operational matters.

Protecting encryption

- The Australian Government should not weaken encryption protocols through any method as a matter of principle.
- The government should focus on the reform of Mutual Legal Assistance Treaties instead of weakening encryption to purportedly improve law enforcement process.

Computer network operations

- There is a need for greater clarity and specificity in law that allow for CNOs in order to comply with democratic norms such as proportionality and rule of law;
- Standards and procedures should be implemented to ensure clarity and transparency in the conduct of extraterritorial investigations, including those involving honeypot or CNOs, with specific regard to ensuring basic standards for determining the admissibility of evidence from remote forms of police surveillance;
- Attempts should be made to improve communications between government agencies under Mutual Legal Assistance Treaties (MLAT) processes, rather than removing these requirements, and the due process procedural safeguards they promote, which has been done via the CLOUD Act

Copyright reform

- The Australian Government should ensure that copyright laws that are flexible, transparent and provide due process to users, through:
  - Include proper due process and privacy safeguards in the website blocking regime.
  - Extension of a safe harbour provisions to all Australian online service providers.
  - Inclusion of a broad, general purpose, 'fair use style' exception to infringement in the Copyright Act 1968.

Content moderation

- Telecommunications providers and internet platforms must develop processes to increase transparency in content moderation by clearly explaining:
  - what content has been removed or triggered an account suspension,
  - who was responsible for making a decision to remove a user's content or suspend their account.
  - why a decision was made (including the specific rule that has been breached).
  - how the moderation system was triggered, including a description of the role of algorithms, other users, law enforcement agencies, other third parties, and internal decision-makers in flagging, detecting, or evaluating prohibited content.

Protecting children online

- Ensure that Australian policy and practice community address all three dimensions of children's rights in relation to the digital world: a) children's access to digital media; b) their rights in online spaces, and how digital media can be harnessed to deliver on a broad range of children's rights.
- Australian research, policy and practice must endeavour to minimise the potential harms and maximise the benefits of online engagement for Australian children. and to adopt a child rights approach to governance, research and program delivery in relation to children's use of digital media.
- Actively engage children and young people in developing responses that protect their rights to provision, protection and participation in the digital age, and develop child-centred measures of impact.
- The rights of disadvantaged children must be centred more consistently across Australian research, policy and practice interventions of online engagement, including investment into research that examines both the potential harms and benefits of children's digital media use.
- Continued support for the eSafety Commissioner's Office and further mechanisms to support cross-sector knowledge sharing; ongoing research; policy development; and evidence-based programmatic responses.
- The Australian Government should lend support to the Case for a General Comment on Children and Digital Media to guide states, NGOs and corporations in their interpretation of the Convention on the Rights of the Child.

Mandatory metadata retention

- Lizzie O'Shea

The Australian Government has introduced a legislative data retention regime that requires telecommunication service providers to retain every customer's metadata for two years[1].

Law enforcement and security agencies can access the data:

- without a warrant or any prior independent authorisation (with the exception of journalists' metadata);
- without a requirement that access is for the purpose of fighting serious crime; and
- without a requirement that a person be informed when their metadata is accessed.

The current regime effectively allows law enforcement bodies to watch everybody, all of the time, without them knowing.[2] While there are some extra protections in place for accessing the metadata of journalists, which require agencies to obtain a special warrant, in at least one case the Australian Federal Police have admitted to unlawfully accessing a journalist's metadata without the relevant warrant[3] and the practical difficulty remains that without looking at the metadata it will not be possible to identify if the metadata is that of the journalist in question. It is not possible for the journalist whose metadata was unlawfully accessed to discover that they are the subject of a breach.

To be consistent with privacy rights, any law concerning the retention of metadata must limit the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted.[4] Australia's data retention scheme is a source of significant concern for civil society organisations.5

There is little transparency around the functioning of the regime, which has very few requirements for public disclosure of requests made or actions taken under this framework.[6] There have been reports that some organisations, including government departments, may be intentionally circumventing privacy protections within the legislation in order to gain access to data that they are not authorised to have.[7] The relevance of such applications to protecting national security is questionable, and these reports serve as evidence of the risk of "scope creep" in such an expansive data collection regime.

The extensive, intrusive nature of the current data collection regime, in combination with a lack of transparency over which bodies are able to access it and for what purposes, risks creating a chilling effect on freedom of expression in Australia and violates the right to privacy.[8]

Recommendation:

The Australian Government should immediately repeal the metadata retention regime or alternatively amend legislation to put in place proper safeguards consistent with the rights to privacy and freedom of expression.

Image: CC Licensed Electronic Frontiers Foundation

Case study: individual access to metadata - the Ben Grubb case

- Angus Murray

The landmark decision in Privacy Commissioner v Telstra Corporation Limited[9] provided judicial guidance on the definition of, and access to, metadata.

In essence, the Full Court of the Federal Court of Australia heard an appeal from the Administrative Appeals Tribunal in relation to a Deputy President of the Tribunal's decision to set aside[10] the Privacy Commissioner's decision to grant a journalist, Mr Ben Grubb, access[11] to all metadata held by Telstra Corp in relation to his mobile phone service. The crux of the matter before the Court was "the very narrow question of statutory construction concerning the meaning of the words "about an individual" as they applied in the Privacy Act prior to 12 March 2014"[12]. The Court maintained a narrow focus on that question and, when dismissing an amici curiae application made by the Australian Privacy Foundation and the New South Wales Council for Civil Liberties, the Court specifically held that "[t]o reiterate: this appeal concerned only a narrow question of statutory interpretation which was whether the words "about an individual" had any substantive operation. It was not concerned with when metadata would be about an individual"[13].

In this context, it is relevant to note the Court's reference to and reliance on Information Commissioner of Canada v The Executive Director of the Canadian Transportation Accident Investigation and Safety Board and NAV Canada where the following paragraph was cited from that judgement:

"The information at issue is not 'about' an individual … the content of the communications is limited to the safety and navigation of aircraft, the general operation of the aircraft, and the exchange of messages on behalf of the public. They contain information about the status of the aircraft, weather conditions, matters associated with air traffic control and the utterances of the pilots and controllers. These are not subjects that engage the right of privacy of individuals."[14]

Telstra made careful submissions in relation to this excerpt and the Court held that "even the utterances of the

Photo: CC Licensed Flickr user monkeyc.net

pilots and controllers, which might identify individuals, were not matters "about" the individuals"[15] with the caveat that "provisions in the Canadian legislative regime considered in The Information Commissioner of Canada case are substantively different from those in the Australian regime"[16]. However, the Court did not provide guidance on the aforementioned differences or the relevance of same before finding that metadata, specifically relating to the operation of mobile services, is not personal information as this term is defined within the Privacy Act 1988 as it is not information "about an individual", instead it is information about a service. This is a particularly important aspect of the decision as the statutory construction of the definition of "personal information" arguably requires information to firstly be about an individual.

The upshot of Privacy Commissioner v Telstra Corporation Limited is that the Court found that metadata is not personal information about an individual if the impugned metadata relates to a service. This finding places Australians in a difficult position as the question of whether metadata is information about an individual who is reasonably identifiable remains unanswered.

As discussed in this report, the implementation of a mandatory data retention scheme in Australia has caused real concern about the impact of the mass collection and retention of metadata. Although Privacy Commissioner v Telstra Corporation Limited has provided judicial guidance on the nature of metadata as it relates to an individual's privacy, it is likely that this decision requires revisiting (in either or both a legislative or judicial manner) with a data subject who has been (or is reasonably capable of being) identified by the aggregation of service-based metadata.

A further issue is the security - or lack thereof - of the data being collected. The legislation does not oblige service providers to retain the data within Australia, and regulatory obligations around security of the data are minimal. Given the high costs of compliance with the legislation, it is likely that service providers will wish to find the cheapest data retention solutions. The potential for theft and misuse is obvious.

Privacy principles

- Dr Tamsin Clarke

Digital rights are an aspect of human rights and include the rights:

- to communicate freely through electronic devices and communications networks, including the internet, without harassment (relevant to freedom of expression[17] and association[18] cultural participation[19] and self-determination[20] and freedom from discrimination[21]);
- to privacy[22] of electronic communication, including the rights to be anonymous, to have one's movements[23] and both the content of one's communications and one's 'digital footprint' kept private, free from collection or surveillance;
- to have control over one's personal data and not have it misused or stolen (rights to privacy, to be free from discrimination[24] and to preserve one's reputation[25]); and
- to have legal redress where one's rights are infringed.[26]

More broadly, the idea of digital rights also encompasses privacy and security issues around the collection and use of information about a person held in digital form, whether that is biometric data, movement data from phones, travel cards, airlines, border crossings or numberplate recognition, to e-health, commercial and financial information.

Breach of digital rights involving "intrusion upon seclusion," such as by physically intruding into a person's private space or by watching, listening to or recording the plaintiff's private activities or private affairs; or "misuse of private information," such as by collecting or disclosing private information about a person, are regarded by the Australian Law Reform Commission as a 'serious invasion of privacy.'[27]

Today, digital rights in relation to free and private communication are essential in order that all human rights can be protected and realised.[28] Indeed many countries have expressed internet access to be a national right. However, digital rights are increasingly restricted by governments, including Australia, in the name of national security. There have been over 66 pieces of counter-terrorism legislation passed in Australia since 2011,[29] with negative consequences for our digital privacy.

Because Australia inherited the English common law, not a civil law, system and did not adopt a bill of rights in its Constitution, Australia does not have a human rights framework to protect digital rights. The Commonwealth Privacy Act[30] is very limited. There is no tort of privacy under Australian law and the common law offers a very inadequate protection for human rights such as privacy. In addition the common law can be overriden by contrary legislation. The result is a 'significant governance gap.'[31]

The Privacy Act regulates collection and use of personal information through thirteen 'Australian Privacy Principles' but does not address surveillance, which is permitted for law enforcement agencies under various legislation.[32] Nor does it apply to Commonwealth intelligence agencies[33] or State or Territory government agencies such as the NSW Police Force.[34] Some States have privacy legislation that regulates use of personal information by State and local government agencies,[35] in some cases involving criminal sanctions.[36]

Even where the Privacy Act does cover law enforcement agencies, there are many exemptions. An entity covered by the Act can only use or disclose personal information for the purpose for which it was collected (the 'primary purpose') unless an exception applies, in which case the entity can also use or disclose that information for secondary purpose(s) (which need not be directly related). Exceptions include use or disclosure which is required or authorised by or under an Australian law or a court/tribunal order (Australian Privacy Principle 6.2(b)). Examples include where:

- a warrant, order or notice issued by a court requires the entity to provide information, or produce records or documents that are held by the entity;
- the entity is subject to a statutory requirement to report certain matters to an agency or enforcement body; or
- a law applying to the entity clearly and specifically authorises it to use or disclose the personal information.

Other exceptions which could be used by law enforcement agencies include:

- Lessening or preventing a serious threat to life, health or safety: (s 16A(1), Item 1).
- Taking appropriate action in relation to suspected unlawful activity or serious misconduct: (s 16A(1), Item 2).
- Reasonably necessary for establishing, exercising or defending a legal or equitable claim: (s 16A(1) Item 4).

Data legally collected by law enforcement agencies can be aggregated with publicly available data, such as from Facebook, to provided a detailed overview of the individual without their knowledge or consent.[37]

The Privacy Act provides for only limited civil redress, by way of complaints to the Australian Information Commissioner.[38]

While Part 5-1A of the Telecommunications (Interception and Access) Act 1979 requires all service providers that collect and retain telecommunications data under the data retention scheme to comply with the Privacy Act in relation to that data, there are no requirements to keep the data in Australia, and it is reasonable to fear that the data could be stolen or hacked.

Recommendations:

In 2014, the Australian Law Reform Commission made extensive recommendations in a document of over 300 pages for the introduction of a Commonwealth statutory civil cause of action for serious invasions of privacy, including digital privacy, following from three earlier enquiries which had supported this reform.[39]

We urge that these recommendations be implemented – which has not occurred to date.

Consumer rights and facial recognition

- Garreth Hanley and Dr Suelette Dreyfus

Shopping centres, advertising companies and retailers are using and investing in new technologies that can collect detailed data about people's movement and behaviours. The data being collected uses a range of new technologies that include physical-biometric identification and mood analysis40 and behavioural-biometrics.[41]

Organisations which collect sensitive data are required to adhere to the 13 Australian Privacy Principles (APPs) outlined in the Privacy Act (Cth) 1988 and are considered an "APP entity". The privacy principles outline the rights of individuals when dealing with APP entities and the responsibilities of entities that collect sensitive or personally identifiable information, including that:

- APP 2 - Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

This principle does not apply if, in relation to a matter, the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.[42]

The use of physical and behavioural biometrics analysis tools removes the right of pseudonymity that individuals have when dealing with APP entities. Behavioural biometrics[43,] a technology that analyses the behaviour of individuals, creates profiles of people that are so unique that businesses are employing it as a security solution to detect behavioural abnormalities and detect digital identity fraud.[44]

When this sensitive data that includes longitudinal behavioural biometrics – or physical biometrics - is collected, stored, or shared for use in big-data analysis, APP entities often state that privacy is protected as the data is often anonymised. However, it has been shown that security through obscurity to protect privacy doesn't work.[45]

The use of biometric analysis technology for security applications being re-packaged and implemented as a tool to monitor the mood of individuals, and their responses to advertising or interactions, it is also being re-purposed to monitor the emotions of employees.[46] This technology is being sold and implemented despite the clear privacy and ethical issues with its implementation, and the questionable value of the measurement itself.[47]

The development of new tools like Cadmus, a tool that claims it can identify potential cheating by university

students using behavioural biometrics, are peering deeper into people's behaviours and collecting detailed individual biometric profiles. The tool is an exemplar of the coalface where the re-purposing of activities, in this case completing assignments at university, to include personal profiling and biometric analysis is occurring.

Cadmus logs the keystrokes of students while they are working, and in doing so records not only the completed work but also each student's individual working style and records the process of working and editing leading up to the completion of their work. The software is cloud based. Itbuilds unique profiles and monitors for changes in typing style, location, and other factors.[48]

The United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, in a report to the UN General Assembly Human Rights Council stated, "Through communications, the most personal and intimate information, including about an individual's or group's past or future actions, can be revealed."[11] Tools like Cadmus take communication surveillance to a new level: the monitoring of the academic working process monitors an individual's self-communication, tracking the evolution of ideas, and effectively monitoring their thinking and working process.

Technologies like Cadmus, that continuously monitor behaviour and communication, can have a stifling effect on free speech and behaviour. When people are being continuously monitored, they are less likely to engage in free speech or free expression, which can lead to under developed personal opinions and the harbouring of fixed views, rather than allowing them to be challenged and developed in the marketplace of ideas.

There has been some commercial rejection of Cadmus; while the software was selected to be trialled at universities across Australia the University of Sydney discontinued use of the software, following complaints from both students and staff.[49] Their complaints were justified as the privacy concerns with Cadmus reflect its infringement of the international human rights framework in relation to privacy, as expressed by the UN Special Rapporteur:

"Privacy can be defined as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals. The right to privacy is also the ability of individuals to determine who holds information about them and how is that information used."[50]

Non-government APP entities operate outside any real regulatory oversight. The regulatory body, the Office of the Australian Information Commissioner (OAIC), can only respond to complaints about privacy breaches, and advise businesses of their responsibilities under the Act. The regulatory approach is one of "voluntary compliance with privacy obligations"[51] and the requirements for APP entities to provide "privacy policies" provides little transparency or specific information about what data is collected or how it is used, with privacy policies often stating that a business "can" or "may' collect and share data. These policies often do not provide information on the right to pseudonymity and ignore the fact that technologies like behavioural biometrics, by definition, limit the rights to privacy under the Act.

Recommendations:

The definition of sensitive information, under the Privacy Act, contains biometric information and biometric templates. The definition of sensitive information must be expanded to specifically include behavioural biometrics.

The right to pseudonymity when dealing with APP entities limits the potential use of biometric data collection in both public or private spaces. Private businesses and other APP entities need to be made aware of their responsibilities under the Act regarding behavioural biometrics, and people need to be informed about, and to maintain, the right to pseudonymity.

The development of a free and easily accessible national "data and movement-tracking opt-out register" for people who do not want their sensitive data to be collected for commercial uses. The register needs to be a single point where people can elect to opt-out of data tracking across all entities easily and without cost.

A compulsory register of entities that collect static and behavioural biometric data needs to be developed. The register should provide the public with information about the entities that are collecting biometric (static and behavioural) data and that have access to such data; the types of data being collected, how the data is being collected, and what entities the data is being shared with.

Any re-purposing of data – provided for one purpose then later used for another – needs to require a process of consent before tasks or accumulated data are repurposed. Consumers need to be made aware of the data being collected and understand what that means for consent to be valid. The use of technologies like Cadmus must be elective, not compulsory, and the extent of monitoring of people's behaviour and communication must be clearly limited by law.

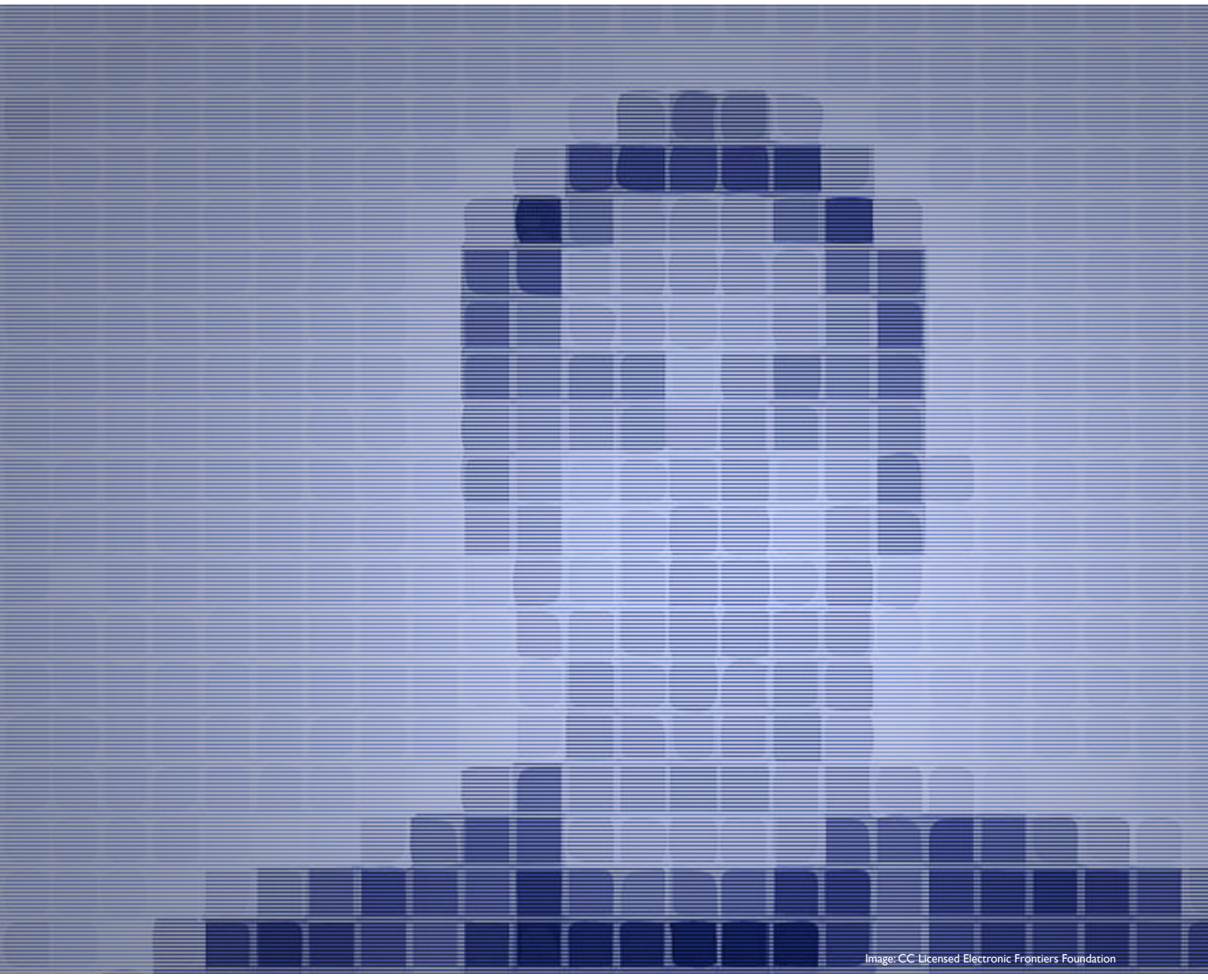


Image: CC Licensed Electronic Frontiers Foundation

Intelligence sharing operations

- Felicity Ruby

The Five Eyes intelligence sharing arrangement among the UK, USA, Canada, New Zealand and Australia began during the Second World War when the UK and US shared technology, techniques in decryption and intelligence derived from breaking German and Japanese diplomatic and military codes. While the technical achievements were kept secret for decades, decoding signals intelligence provided insight into enemy weapons capabilities and battle plans, giving strategic advantage to the western allies that changed the operational course of the war.

The continuation of war time practices into the post-war environment was formalised on 5 March 1946 with the signing of the UKUSA Agreement,[52] expanded in 1947 to include Canada, Australia and New Zealand as "UKUSA-collaborating Commonwealth Countries", with these conveniently located dominions of the British Empire known also known as Second Parties or, as Stephen Lander once overheard a US intelligence chief calling them, "islands with aerials."[53] However, the alliance is not one agreement made back in 1947, but an estimated several hundred supplementary 'ties that bind'[54] in the form of ongoing technical arrangements, working practices, operating procedures and relationships that are dynamic, subject to change and designed to standardise and prioritise the information flow to the US.

The 1985 study of the Five Eyes by Jeffrey Richelson and Desmond Ball describes it as, "one of the largest bureaucracies in the world… a truly multinational community, with its numerous organisations and agencies bound together by an extraordinary network of written and unwritten agreements, working practices and personal relationships… able to shroud itself in secrecy and to invoke the mantle of 'national security' to an extent unmatched by even the national defence establishments."[55] Nicky Hager's groundbreaking 1996 study of the Five Eyes Echelon system revealed that it draws down all enciphered and open communications from satellites encircling the globe in space, and also from fibre optic cable, for bulk decryption and analysis through a software system called The Dictionary that could 'read every word and every number in every single incoming message… pick[ing] out the ones containing target keywords and numbers."[56]

At its core, the arrangement commits each party to gather signals intelligence in their designated geographic zone and to share, "almost everything from the raw take to their finished analytical products and the equipment, services and secrets that fed into their production."[57]

Australia is usefully located in ideal listening range of South East Asia, as well as of large parts of Russia and China. That is, facilities in Australia and Australian agencies are key in extracting and analysing the communications of countries in our region – all Indonesian communications, for example. Australia's location in relation to the US is also an important consideration, as facilities in the US and Australia combined offer global coverage for military and surveillance operations.[58] Sparsely inhabited expanses of Australia's deserts and coastline are particularly useful for clear interception of electronic emissions picked up by satellites and beamed back to earth.

It is difficult to identify offices, training grounds and minor facilities owned, used, leased and occupied for Five Eyes purposes in Australia as many are concealed under dual or temporary use arrangements, however, the major

facilities include the Shoal Bay receiving station outside of Darwin, the Kojarena defence satellite communication facility near Geraldton in Western Australia, the North West Cape naval communications station also in Western Australia and the Pine Gap joint facility near Alice Springs, which plays a vital role in intelligence collection, increasingly battlefield intelligence and drone targeting.

The Australian agencies that have direct Five Eyes functions, responsibilities and activities include Australian Signals Directorate (ASD, formerly known as Defence Signals Directorate or DSD), the Defence Intelligence Organisation, Australian Secret Intelligence Service (ASIS) and the Australian Federal Police, however, the number of departments and agencies engaged on a particular project or operation, or for a short duration, is unknown.

The scope of cooperation is growing, as then Attorney General Senator George Brandis disclosed on 22 February 2016 using the parliamentary device of a Dorothy Dixer, a question by the government to the government, to inform the listening public about a Five Eyes meeting held in Washington DC the previous week, which included, "Attorneys-general, national security ministers and, for the first time, immigration ministers" to increase information sharing about the flow of migrants, a topic now apparently more firmly on its agenda.[59] Unconfirmed rumours currently circulating allude to a further formalised expansion of collaboration and intelligence sharing between police agencies among the Five Eyes.

At the height of the Cold War, Professor Desmond Ball asserted that successive Australian governments had shrouded surveillance agencies, facilities and decisions in more secrecy than their Five Eyes partners, showing less regard for the privacy rights of Australians and more aggressively quashing peaceful democratic resistance. At least the very existence of Australia's main Five Eyes participating organisations is no longer secret, with the ASD (established in 1947, acknowledged in 1977), ASIS (established in 1952, acknowledged in 1977), ASIO, ONA and DIO all having public websites with some announcements and documents occasionally made available officially. It is worth noting that none of these organisations, or any Cabinet level security decisions or papers is subject to Freedom of Information requests, which is not the case in the USA, where both CIA and NSA documents can be requested. In addition, the oversight function of the Parliamentary Intelligence Committee is closed to public view and the committee is not permitted to examine "the intelligence gathering and assessment priorities", or "sources of information," but is limited in its oversight to administration and expenditure questions.

The legal barriers to accessing information from current and former staff of intelligence agencies are significant given they are bound by the strict penalties outlined in Part 6 Division 1 on Secrecy in the Intelligence Services Act as well as other laws that prohibit the disclosure and communication of certain information, or even the publication of the identity of staff. Non-disclosure provisions of the Intelligence Services Act also bind members of the Parliamentary Committee and the staff that support them. Another significant development was the passage of the National Security Legislation Amendment Act of 2014, under which

anyone disclosing information about a 'special intelligence operation' can go to jail for five years, even if that person hasn't realized that the information disclosed was related to a special intelligence operation.[60]

Edward Snowden patiently explained – initially to three aghast journalists in a Hong Kong hotel room, and through them to the world – the significance of multiple and simultaneous technical and commercial programs that place backdoors into software and hardware, rendering much online infrastructure vulnerable to attack - from cell phone devices to server stacks and email clients to payment mechanisms. Browsers are infected. Encryption standards have been deliberately weakened. Submarine optical fibre cables have been tampered with and tapped. Even offline devices can be 'illuminated' and their data read. With the evidence provided by Snowden we know the entire Internet is 'owned' by the NSA and its Five Eyes partners, including all the networked devices in the hands of individuals, heads of state and their spouses included, and corporations are along for the ride, willingly or unwittingly.

Amidst the noise arising from the revelations, there has been very little haste towards reform. Judicial, legislative and executive power over the Internet remains where it was in June 2013. Attempts at policy reform in the Five Eyes jurisdictions have conclusively failed. While the states responsible were rattled, their response has been to accelerate legislative mandates through their respective parliaments, with the effect of actually increasing mass surveillance and its legitimacy.[61] Some of the intermediary companies have been embarrassed enough to attempt protection of clients and users through increased security and encryption[62], however, the surveillance apparatus and practices Snowden exposed continue unabated. Indeed, former National Security Agency chief Michael Hayden mocked the pace of reform at a June 2015 Wall Street Journal event, celebrating the failure of resistance with the comment, "And this is it after two years? Cool!"[63]

The Australian parliament passed legislation instituting mandatory data retention and jail terms of up to 10 years for journalists reporting on special operations, which in the Attorney General's own words, was, "primarily intended to deal with an Edward Snowden type situation." Under the National Security Legislation Amendment Bill of October 2014, ASIO can obtain intelligence from a number of computers (including computer networks or indeed the whole Internet) under a single warrant. With passage of the Counter-Terrorism Legislation Amendment (Foreign Fighters) Bill in October 2014 the legality of tracing a suspect's Internet activity was strengthened, with the Australian Federal Police (AFP) gaining increased access to data held on computers without notifying operators. Under the Telecommunications (Interception and Access) Amendment (Data Retention) Bill of March 2015 all telecommunications and Internet providers are now forced to store metadata on all Australians for two years. Within 8 weeks of its passage, the list of agencies with access to metadata was increased to include the Australian Border Force. With the passage of the Copyright Amendment (Online Infringement)Bill in June 2015, rights holders are now able to force Internet Service Providers to block overseas websites – effectively an Internet filter. The 2017 National Intelligence review proposed that Australia create a new senior bureaucratic position of Director General of National Intelligence, primarily because the other Five Eyes countries have one.

Since the Snowden revelations, no complicit government official or company partner has been disciplined or dismissed for illegal surveillance or overreach. Lying under oath has been forgotten or forgiven. Despite the Obama administration welcoming the debate he sparked, Snowden alone has been charged with crimes of espionage and stealing government property. As much as he has been condemned as a traitor and worse, Snowden has also been showered with awards and opportunities to educate, enrol and explain his case. In a statement marking the second anniversary of his disclosures, he admitted to fearing "public indifference or practiced cynicism", but celebrated the "power of an informed public" and asserted, "…the balance of power is beginning to shift,"[64] although there haven't been many signs of that in Australia.

Routine mass surveillance practices of these five democracies have provoked questions about what is legitimate or arbitrary surveillance power and whether democratic intelligence is a possibility or an oxymoron. To propose that indiscriminate intelligence collection and sharing can be corrosive of democracy is not to deny a legitimate role for secrecy and surveillance powers in the hands of law enforcement, national security and surveillance agencies. Democratic scrutiny, judicial warrants, Ministerial accountability, and Parliamentary oversight are all measures designed to protect those agencies with the authority and legitimacy of social licence as much as they are designed to protect the public from overreach.

Intelligence collection and sharing is not a necessary evil or something to be discarded outright. Former British intelligence officer Michael Herman has noted that, "in the field of intelligence, international exchanges are a necessity for international society," and that, "The idea of ethical foreign policy got a bad press when given political salience in Britain in 1997, but was in reality a statement of the obvious. Intelligence has to fit into the ethics of an increasingly cooperative system of states, perhaps with bigger changes in thinking than have previously seemed possible."[65]

As noted by Patrick Walsh and Seumas Miller in their effort to rethink Five Eyes intelligence collection policies after Snowden, "there is a need to develop ethically informed sets of policy guidelines to guide policy making on improving security intelligence collection in liberal democratic countries whilst managing the risks associated with it."[66] But as David Horner's official history of ASIO often showed, successive Australian governments have (not always) recognised the need for these agencies to be free from political interference and domestic political agendas, vendettas or party preoccupations.[67] This is particularly relevant when considering the impact of surveillance on social movements, and the history of intelligence and security agencies conflating activism with terrorism in Australia.

Recommendations

The loopholes opened with the 2011 reform of the FOI laws should be closed by returning ASD, ASIO, ASIS and other intelligence agencies to the ambit of the FOI Act, with the interpretation of national security as a ground for refusal of FOI requests being reviewed and narrowed.

Warrantless surveillance erodes the social licence and reputations of law enforcement, national security and intelligence agencies, who need a warrant to enter our homes and should also need one to access our telecommunications data.

A new agreement is needed among the Five Eyes that any information held by the United States on nationals of the other countries be stored only within the borders of that country and unless directly related to a national security operation or criminal trial, be accessible only with the approval of the home government, with an annual report of how many requests for access have been made.

Commercial espionage to benefit Australian companies and those of other Five Eyes countries conducted by ASD and other agencies is misuse of security, intelligence and law enforcement capacity and must cease.

Australia's Joint Parliamentary Committee on Intelligence and Security has been given extended powers to "initiate its own inquiries" under the 2017 National Intelligence Review, however, that power is limited only to "the administration and expenditure of the ten intelligence agencies of the NIC as well as proposed or existing provisions in counter-terrorism and national security law, and to review all such expiring legislation." The committee should also be able to initiate its own reviews into operational matters.

Protecting encryption

- Lizzie O'Shea and Elise Thomas

Encryption plays a major role across many important areas of Australian life, including national security interests, the economy, and protecting the community, individuals, service providers, and the private sector from crime and other risks.

Encryption is a method for ensuring communications between two parties remain private from everyone else, including the carrier. Even if an encrypted communication is intercepted by a third party, it cannot be read by anyone except the people who are authorised to decrypt it. Encryption is a foundational tool for the proper functioning of the digital society and economy, and is used in a wide range of settings, including banking, public service delivery, and communications systems.

At various times governments have attempted to regulate encryption, with little success. Most recently in the UK, the government has introduced the Investigatory Powers Act[68], which requires technology companies to assist the government to decrypt messages where technically feasible[69]. It is unclear what this provision means in practice for companies and individuals that rely on encryption. The Act is still being implemented, so it has not yet been possible to observe how it will be used.

Prime Minister Malcolm Turnbull has stated that his government wants to introduce a method for intercepting and reading encrypted messages. In July 2017, he discussed giving law enforcement this power for the purposes of keeping the public safe from terrorism. In that same press conference, then Attorney General George Brandis argued that the government's surveillance powers needed to be brought up to date by requiring that technology companies cooperate with law enforcement. Attorney General Brandis indicated that this initiative is part of Australia's participation in the Five Eyes, and confirmed the government's commitment to intelligence sharing with these partners.

It is not clear how the government plans to implement these changes in law. This uncertainty suggests that the government does not appreciate the complexity of the issues involved. Approaches proposed or used in other countries include outright prohibitions on encryption, escrow of encryption keys, or limitations on the strength of encryption. Each of these has been demonstrated to have serious risks. Two of the most commonly discussed options in Australia have been to require technology companies to build a 'backdoor' to allow direct government access, or, conversely, to obligate companies to build into systems the capacity to decrypt the messages and then hand the information over to the government. Attorney General Brandis indicated that mandating a backdoor is not the government's plan, however he also stated in June 2017 that 'if there are encryption keys then those encryption keys have to be put at the disposal of authorities.'[70]

The reactions from experts and commentators have highlighted deep problems with the government's general plan. Academics have outlined the flaws from an engineering perspective. 'Decrypting terrorists' communications without undermining the security of everyone else sounds great,' wrote academics from the University of Melbourne, 'but this is not an engineering plan and every known attempt has failed.'[71] Built-in weaknesses in encryption systems are not features that

can be exploited only by the government; they can also be used by criminals and foreign enemies. Information about any backdoor will be highly valuable, and a honeypot for hackers, making it hard to keep safe. In July 2017, private health insurer Bupa notified tens of thousands of their customers that their private information had been leaked by a rogue employee[72] – demonstrating the immense security risks facing institutions charged with protecting data. Journalists have also pointed out that the proposal is unlikely to be effective for its intended purpose: terrorists can, and likely will, move to other communication channels that have strong encryption[73]. Civil society organisations have argued that police already have significant powers to investigate terrorism and this proposed extension of surveillance capabilities has not been justified.[74]

The government's Digital Economy Strategy[75], Cyber Security Strategy[76], and International Cyber Engagement Strategy[77] each confirm the importance of digital technologies and cyber security for Australia in the years ahead. Encryption is a crucial element of all cyber security strategies. The purpose of this paper is to demonstrate that encryption is essential to the digital society, and encryption is only effective if it is robust. A system of encryption with a back door is like a chain with a fatally weak link – the strength of the entire system is compromised and it is only a matter of time before it breaks, jeopardising the safety of everyone who relies on it. This risk has profound implications for systems and infrastructure that we rely on for our daily lives.

The Turnbull government has expressed concern about terrorists using encryption to evade surveillance, but this concern misses some important considerations. The case for weakening encryption has not been made out, especially in a context in which so many everyday digital activities would be put at risk. The government's job is to develop policies that protect national security without endangering public safety and economic interests. The focus on weakening encryption does not meet these requirements.

In seeking to achieve the stated aims, the government should investigate the use of Mutual

Legal Assistance Treaties (MLATs) between Australia and other countries include arrangements for information sharing for law enforcement purposes. These processes tend to be slow, opaque, and inefficient. Reform of MLATs is an urgent priority to ensure that intelligence is shared in a timely and effective manner. It would allow intelligence agencies to make better use of evidence they already have, rather than encourage them to seek access to evidence they do not yet have (like encrypted messages). The reform of MLATs ought to be a focus of the government.

Recommendations:

The Australian Government should not seek to weaken encryption protocols through any method as a matter of principle in upholding the security of those protocols.

The government should focus on the reform of Mutual Legal Assistance Treaties (MLATs) instead of weakening encryption to purportedly improve law enforcement process.

Digital rights in the workplace

- Melanie Poole

Australian workers should be worried about our digital rights. We currently have a flimsy and limited patchwork of privacy and surveillance protections, mostly drafted in the 1980s before the internet even existed. Under our laws, it is broadly permissible for employers to digitally spy on workers, even outside of work hours. This not only threatens workers' right to privacy, but also our right to freedom of political communication. If employers can control what their workers do and say online outside of work hours, it undermines the right of anyone who is not a member of the capitalist class (i.e. an employer) to participate in public and political debate. This fundamentally puts our democracy at risk.

There is currently no statutory 'right to privacy' in Australia. Employers have to abide by the "Privacy Acts" – a mix of Federal and State legislation that covers the collection, use and disclosure of personal information about individuals. But these Acts only place broad limitations on how data about individuals can be used – they do not establish a fundamental right to privacy, nor specifically cover the issue of workplace surveillance.

New South Wales and the Australian Capital Territory are the only jurisdictions that have specific protections concerning digital surveillance in the workplace. Victoria also has surveillance legislation, but it only covers surveillance in places such as bathrooms and doesn't cover digital rights.

In NSW and the ACT, employers are allowed to conduct surveillance on workers while they are at work. The surveillance has to be for the purpose of monitoring how they are doing their job. This includes monitoring their use of mobile phones, computers and other devices, if these are used for work. Surveillance cannot be secret, however this is not hard to get around: the employer just needs to have a policy that gives workers notice of the type of surveillance they will be under.

Technically, in NSW and the ACT, employers cannot monitor workers outside of work. But there is an exception when employees are using the employer's resources. Given that the nature of work is rapidly changing, with flexible working arrangements more common and workers in many professions expected to use phones, laptops and other devices provided by employers in order to be constantly reachable, this exception is worryingly broad.

Across Australia, employers can:

- Monitor the use of email, the internet, social media and other computer resources. This includes monitoring not only of the computers or other devices owned by

the employer, but even workers' own devices if used for work purposes or connected to work internet.

- Monitor use of personal social media outside of work hours. All that employers have to show is that the social media monitoring either relates to the worker's employment OR to "conduct that is not condoned by the employer."

This means that workers have very limited protections if their personal information is used by employers as grounds for disciplinary action or dismissal.

While the Fair Work Commission (FWC) has not questioned the ability of employers to conduct surveillance both inside and outside the workplace, they have placed limits on the extent to which the data collected can be used to dismiss workers. The following precedents have been set in recent times through various cases brought before the FWC.

An employer has to adequately draw attention to its IT policies, and action them in a reasonable time period. In 2013, the FWC found that three Australia Post employees who had used their work email to send and receive pornography could not be dismissed, because Australia Post had not made employees aware of its IT policy, or taken action against noncompliance for a long period.[78]

Employers have to be clear about how they will conduct surveillance. In 2014, a worker sacked from the Department of Defence for excessive internet use was deemed to have been unfairly dismissed due to the Department's "vague and contradictory" IT policies.[79]

Comments made by workers on their personal social media have to result in actual reputation damage. In 2016, the FWC concluded that the comments made on social media by Starr, an Australian Public Service employee 'even if they are offensive, made in a private capacity but which relate to work, are not sufficient grounds for the termination of employment in the absence of some actual (rather than perceived or potential) reputational damage to the employer'.[80] As a public servant, Starr was covered by the Australian Public Sector Commission's employee social media guidelines.

"Foolish" comments aren't enough to justify dismissal, but Facebook posts can be treated as public. In 2010, an employee wrote on Facebook: "Xmas 'bonus' alongside a job warning, followed by no holiday pay!! Whoooooo! The hairdressing Industry rocks, man!!! AWESOME!!!" The Fair Work Commission found that, while 'foolish and silly in the context of them being made on a public forum', the comments did not justify dismissal.[81] However, the Commissioner did say in making the judgment that, given

the nature of posting online and the fact the audience to a comment cannot be controlled, '[it] is no longer a private matter but a public comment' and that 'it would be foolish of employees to think they may say as they wish on their Facebook page with total immunity from consequences'.

In analysing the state of affairs within Australia, there are several lessons that we should learn from overseas jurisdictions who have tackled these issues.

In 2017 French labour laws established a "right to disconnect". Employers with at least 50 employees must outline, as part of their mandatory workplace bargaining agreement, how they will regulate the use of digital tools to make sure that this does not encroach on statutory periods of rest and holidays.

The law does not define the 'right to disconnect' – it allows each employer to create appropriate regulations through negotiation with its union delegates or staff representatives, taking into consideration the nature of the work their employees do. But employers must draw up a "charter" for the proper use of digital tools, acknowledging the "right to disconnect" and how it will be protected. They also have to provide training and awareness-raising actions for all staff to ensure "the reasonable use of digital tools".

The incentive for employers to implement the right to disconnect is strong: failure to do so opens them up to the risk of significant civil liabilities, such as salary back payment for overtime, damages related to health conditions (depression / burnout / psychological harassment) and/or to penalties for non-compliance with statutory rest and holiday periods.

The right to disconnect is not the complete answer to Australia's current lack of digital workplace rights protections – it doesn't, for example, create a right to privacy – but it would go a significant way to stopping the expansion of employer control in workers' private lives. This sends an important signal, both legal and social/cultural, about the limits of employer control over workers' lives.

Sweden, Denmark and Norway all have government-run Data Protection Authorities, which work to protect privacy. As part of the European Union (EU), Sweden and Denmark are covered by the European Data Protection Supervisor, which monitors how well member states follow the EU's General Data Protection Regulation (GDPR) (2016). The EU's response has been more proactive than Australia's response: European law has long recognised the fundamental right to privacy and to data protection.

Given the weakness of Australian privacy laws regarding digital rights in the workplace, it would likely be a major improvement to create a similar body to the Data Protection Authorities – tasked with upholding and monitory privacy protections, including digital rights in the workplace. It is worth noting, however, that the GDPR does not prevent employers from monitoring workers while they are at work.

In 2016, the European Court of Human Rights ruled on the case of a Romanian engineer fired for sending messages to his fiancée and brother in an online chat program installed at his employer's request.

Bogdan Mihai Barbulescu's digital communications were monitored for eight days, during which time his employer recorded a 45-page transcript of messages about personal issues, including "his health and sex life". Barbulescu argued his employer violated his right to correspondence and his emails were protected by his right to privacy. But the court found he had been warned of the company's computer use policy, and businesses should be able to "verify that employees were completing their professional tasks during work hours".[82]

The ruling sets a precedent for all European workplaces, and it is likely that, where employers can prove that they have made workers aware of their computer use policies, and are conducting surveillance for the purpose of ascertaining work performance, surveillance will be allowed.

Australian workers are in an increasingly vulnerable position when it comes to our digital rights in the workplace. As the nature of work changes, and becomes less confined to traditional 9-5 timeframes and static office locations, there is a very real risk that the extent to which employers are permitted to control workers' lives will expand. The increasing number of cases involving workers losing their jobs because of comments made on their personal social media accounts, in their own time, is evidence of this.

If we are to aim for real progress in this area, what is required is a multi-sector campaign that demands better digital rights protections for workers. The vast majority of Australians support the right to privacy: they do not, for example, think that employers should look at their employees' social media pages.

We are facing a critical decade, during which we will see the nature of work rapidly transform. Without strong digital rights protections for workers, the risk is that digital technologies will be used to facilitate a transfer of power from workers to employers, to chip away at core human rights such as the right to privacy and the right to freedom of political communication, and to fundamentally weaken democracy. But we still have time to change this: and the steps taken in France and Scandinavia give us a great place to start.

Recommendations:

The Australian Government should introduce legislation that respects and upholds the right to digital privacy and to data protection.

Investigate the creation of a similar body to the European Data Protection Authorities and task this body with upholding and monitory privacy protections, including digital rights in the workplace.

Explore the possibility of a 'right to disconnect' that would regulate employer's use of digital tools to make sure that this does not encroach on statutory periods of rest and holidays of employees.

Computer network operations and cross-border data requests

- Drs Monique Mann, Adam Molnar & Ian Warren

As digital communications routinely traverse transnational jurisdictions, criminal investigation and surveillance practices raise novel challenges for the protection of human rights. The emergence of Computer Network Operations (CNOs) (more popularly termed as 'hacking') as well as lawful data access requests via third party intermediaries outside the scope of traditional Mutual Legal Assistance Treaties (MLATs), are both redrawing the boundaries of many rights preserving conventions. Our research[83] has shown that new online investigations and transnational surveillance practices require clear standards to avoid the prospect of criminal investigations becoming unilateral enforcement decisions without independent judicial oversight. This will ensure the admissibility of evidence, support accountability, and will protect human rights.

Computer Network Operations (CNOs) in Australia

Australian law enforcement agencies (LEAs) are engaging in Computer Network Operations (CNOs) as an investigatory or intelligence gathering method. CNOs entail electronic intrusion and/or interference with equipment associated with network infrastructures, such as servers and routers, and 'end-points', such as mobile devices and computers. Current use of CNOs in Australia raise serious concerns about proportionality, due process, human rights, and the security of information communication infrastructures. This is in part because current legislative authorisation for CNOs is ambiguous, and provides widened scope for CNOs in the absence of a formal bill of rights. For instance, under 2014 amendments to the ASIO Act (1979) (Cth), the legal definition of a "computer" has been broadened to include "one or more computers", "one or more computer systems", "one or more computer networks", or "any combination of the above". The result is that a single warrant issued through executive authorisation by the Attorney-General could, in principle, be used to search or interfere with entire businesses, telecommunications companies, or core internet infrastructure.

CNO investigations routinely extend extraterritorially, as LEAs take over illegal marketplaces and networks to collect information from all over the world. This can involve seizure of offending websites and subsequent hosting on law enforcement servers to deploy malware to identify visitors around the world. While the legality of these processes is unclear and subject to ongoing litigation in the US, Australian LEAs involved in child exploitation investigations have mirrored international trends (i.e. 'Operation Pacifier' into the 'Playpen' network). For example, in 2014, the Queensland Police Service 'Task Force Argos' operated a site used for the distribution of child exploitation material as a 'honeypot' to unmask IP addresses of visitors to the site. At present, there is limited regulatory guidance for the use of extraterritorial CNO procedures in any jurisdiction, and decisions to deploy CNOs are seldom open to independent judicial oversight or review until a prosecution has commenced.

Cross-border data requests: MLATs, Microsoft Ireland and the CLOUD Act

The transnational nature of the internet and electronic data flows introduce novel challenges for criminal law, its enforcement, and relevant due process protections that are delineated according to the principle of territoriality. Most internet and cloud computing services are administered by US corporations. At present the US government has resolved this issue by legislating to enable digital evidence that is located outside of the US, which remains under the control of US corporations, to be accessed directly via the companies themselves rather than through MLAT processes with relevant government authorities. It is unclear if Australia will be one of these countries, but given close previous relations with the United States, this is likely to be subject to negotiation in the coming years.

The Microsoft Ireland case would have determined whether US federal authorities could lawfully access data stored by Microsoft in a server located in Ireland, outside of MLAT procedures. MLATs are a formally recognised structure for the exchange of evidence between government agencies in two or more jurisdictions. They can be cumbersome with potential to impede the collection of digital evidence, yet they are important instruments to protect individual and due process rights, and to ensure evidence is admissible in domestic criminal trials. The Microsoft case was rendered moot when the Clarifying Lawful Overseas Use of Data (CLOUD) Act was passed in 2018. How these data sharing agreements will operate to sidestep existing legal safeguards provided through MLAT procedures remains to be seen, but this development has considerable potential to undermine existing foreign privacy protections.

Recommendations:

There is a need for greater clarity and specificity in law that allow for CNOs in order to comply with democratic norms such as proportionality and rule of law.

Standards and procedures should be implemented to ensure clarity and transparency in the conduct of extraterritorial investigations, including those involving honeypot or CNOs, with specific regard to ensuring basic standards for determining the admissibility of evidence from remote forms of police surveillance.

Attempts should be made to improve communications between government agencies under Mutual Legal Assistance Treaties (MLAT) processes, rather than removing these requirements, and the due process procedural safeguards they promote, which has been done via the CLOUD Act.

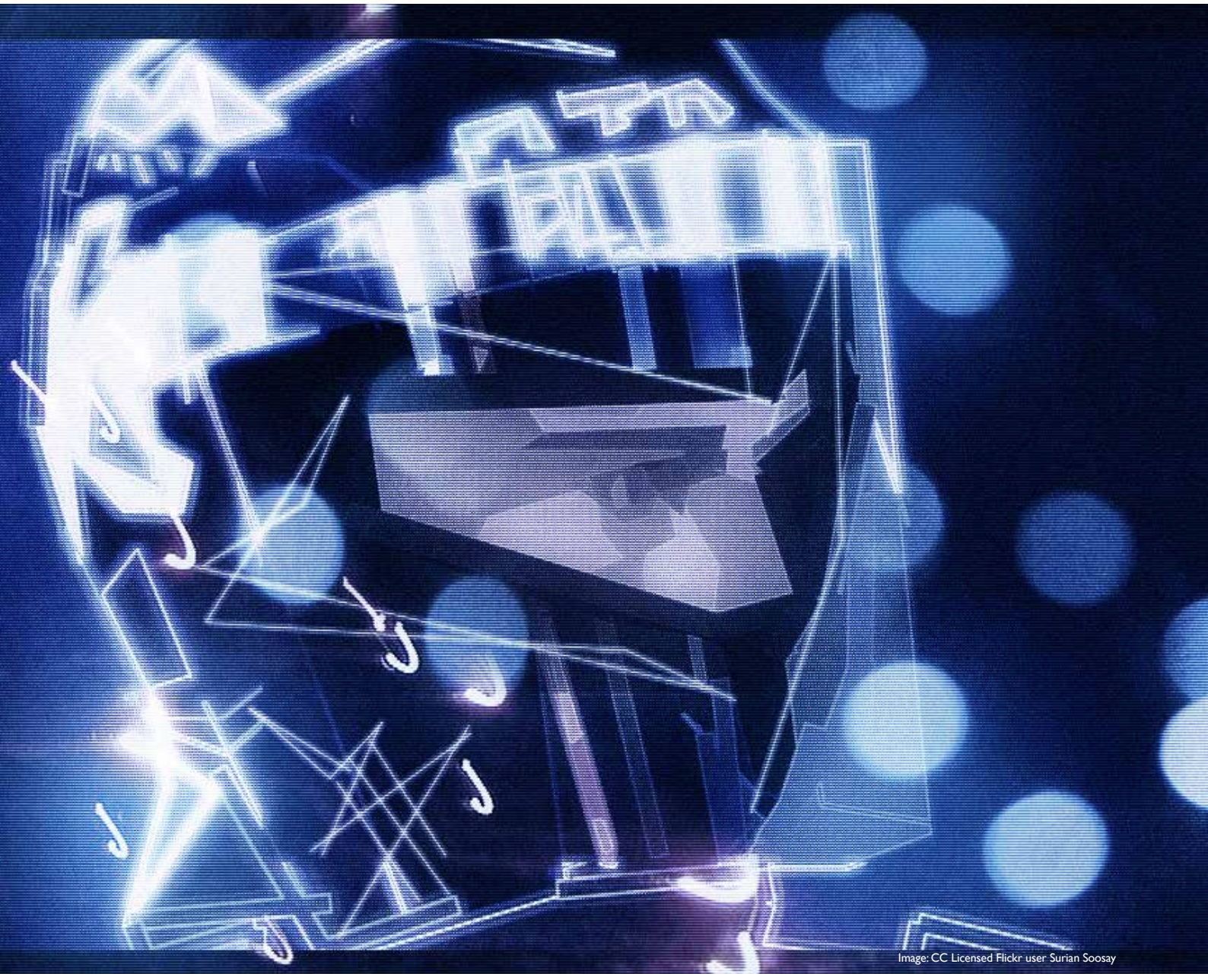


Image: CC Licensed Flickr user Surian Soosay

Case study: automation of government welfare services

- Gillian Terzis

Australia is somewhat unique in that the vast majority of its welfare benefits are means-tested. The consequences of this are complex. On the one hand, Australia's welfare system is narrowly targeted toward low-income earners, giving the government more bang for its buck—welfare provisions make up a much lower proportion of its GDP than other OECD countries. The rationale behind means testing is to encourage fairness in the welfare system, ensuring that people receive what they are entitled to. Anyone who falls afoul of the system's stringent requirements must pay back their "debt" to the government.

This "debt"—the difference between what you receive and what you are supposed to receive—is the root of the 'robo-debt' scandal. The scandal's origins date back to 2011, when the Australian Labor Party introduced a data-matching algorithm officially known as Online Compliance Intervention. Its purpose was to compare the earnings reported by welfare recipients to the social services agency Centrelink with the earnings reported to the Tax Office by their employers. Discrepancies would be investigated by Centrelink staff members, who would then decide whether to follow up with the recipient by letter or phone.

In December 2016, the government announced that the system had undergone full automation. Humans would no longer investigate anomalies in earnings. Instead, debt notices would be automatically generated when inconsistencies were detected. The government's rationale for automating the process was telling. "Our aim is to ensure that people get what they are entitled to—no more and no less," read the press release. "And to crack down hard when people deliberately defraud the system."

The result was a disaster. Checking in to a MyGov account only to find hundreds or thousands of dollars in arrears, supposedly due to inaccurate reporting of income. Threats from private debt collectors, who told people their wages would be seized if they didn't submit to a payment plan. Those who wanted to contest their debts had to lodge a formal complaint, and were subjected to hours on hold before they could talk to a case worker. Others tried taking their concerns directly to the Centrelink agency on Twitter, where they were directed to calling Lifeline, a 24-hour hotline for crisis support and suicide prevention. As coverage of the robo-debt scandal spread, calls for the government to suspend the scheme mounted. Yet it refused to halt the program until an inquiry by the Australian Senate finally ordered it to do so in May 2017

Automation is dehumanizing in a literal sense: it removes human experience from the equation. In the case of the robo-debt scandal, automation also stripped humans

of their narrative power. The algorithm that generated these debt notices presented welfare recipients with contrasting stories: the recipients claimed they'd followed the rules, but the computer said otherwise.

There were few official ways to explain one's circumstances: twenty-nine million calls to Centrelink went unanswered in 2016, and Centrelink's Twitter account seems explicitly designed to discourage conversational exchange. One source of narrative resistance is notmydebt.com.au, a website run entirely by volunteers that gathers false debt stories from ordinary Australians so that the "scandal can't be plausibly minimised or denied."

Over time it was revealed that many of these debts were miscalculated or, in some cases, non-existent. One man I'd read about was on a government pension and saddled with a $4,500 bill, which was revised down months later to $65. Another recipient, who was on disability as a result of mental illness, had a debt notice of $80,000 that was later recalled. A small proportion of recipients were exclusively in contact with private debt collectors and received no official notice from Centrelink at all.

Soon it emerged that social services were a lucrative avenue for corporate interests: this year's Senate inquiry revealed that some private agencies tasked with recouping debts were working on a commission basis, pocketing a percentage of the debts they had recovered for the government regardless of their validity. (All debt notices issued by private agencies were eventually rescinded after government review in February 2017.)

The methodology of the algorithm itself was riddled with obvious flaws. It calculates the average of an individual's annual income reported to the Australian Tax Office by their employer over twenty-six fortnightly periods and compares it with the fortnightly earnings reported to Centrelink by the welfare recipient. All welfare recipients are required to declare their gross earnings (income accrued before tax and other deductions) within this fourteen-day period. Any discrepancy between the two figures is interpreted by the algorithm as proof of undeclared or underreported income, from which a notice of debt is automatically generated.

Previously, these inconsistencies would be handled by Centrelink staff, who would call up your employer, confirm the amount you received in fortnightly payments, and cross-index that figure with the one calculated in the system. But the automation of the debt recovery process has outsourced authority from humans to the algorithm itself.

It's certainly efficient: it takes the algorithm one week to generate 20,000 debt notices, a process that would take up to a year if done manually. But it's not a reliable method of fraud detection. It's blunt, unwieldy, and error-prone. It assumes that variations in the data sets are deliberate, and that recipients have received more than what they are entitled to. What's more, the onus is on the welfare recipient to prove their income has been reported correctly and that the entitlements they have received are commensurate, within twenty-one days.

Yet, as many critics have noted, this income-averaging method is porous. It fails to accurately account for the fluctuating fortunes of casual or contract workers, which often results in variations between the two figures. Variations also inevitably arise because recipients are required to register their income with Centrelink not for periods that are past, but for current periods that end a number of days in the future. Casual or contract workers who do not know what work future days will bring them therefore regularly need to correct their work estimates - a process which is made extremely difficult, whether by computer, phone or in person. There's also no way for the algorithm to correct for basic errors in the system's database. It cannot yet discern whether an employer's legal name has been used instead of its various business names—it treats them as separate entities, and therefore separate sources of income—or whether conflicting reports are caused by basic mistakes, such as spelling errors or typos.

These seemingly small distinctions are ones that only a human could make. It's no wonder, then, that conservative estimates of its error rate hover at 20 percent.

Centrelink's automated debt recovery program is part of an ongoing initiative to expand the range of essential government services provided to Australians online. In an interview with ABC Radio National, the Australian national public broadcaster, Prime Minister Malcolm Turnbull referred to this digital shift as an "important part of the government's productivity agenda," and promised it would ensure that "citizens can engage with government on digital platforms as easily and conveniently as they do with their banks or e-commerce vendors." It's the kind of market logic that treats Australians as little more than consumers.

What the scandal shows is that the neutrality of technology is a fallacy. A tool is only as good as the politics that underpin it. It's not an accident that the Australian government's attempt at algorithmic governance was inhumane. It was a defining feature of its design.

Photo: CC Licensed Flickr user David Jackmanson

Copyright

- Dr Kylie Pappalardo and A/Prof Nicolas Suzor

Recent years have seen some positive amendments to Australian copyright law, particularly in improving access to information and cultural goods for Australians with a disability. Importantly, however, the Australian Government has not yet acted upon successive recommendations to improve the operation of copyright law for ordinary Australians through the introduction of a flexible 'fair use' exception to infringement. We also note with concern the limited due process protections available for Australia's website blocking regime, and the lack of protection available for Australian hosts of user-generated content under the safe harbour regime.

ISP liability and the website blocking regime

In 2012, the High Court of Australia held that iiNet, an ISP, had no legal duty to police what its subscribers did with their internet connections. The litigation was brought by a coalition of rights-holders seeking to enforce their copyright by holding the ISP responsible for alleged customer infringements committed by downloading films via BitTorrent.[84] The court found that ISPs are under no general obligation to take measures against subscribers based only on the strength of copyright infringement allegations made by rights-holders.

After this decision, copyright owners shifted tacks - they sought not to hold the ISPs themselves liable for copyright infringement, but rather to compel cooperation from ISPs in handing over customer data.[85] In April 2015, the Federal Court of Australia granted judgment in favour of the rightsholders of the 2012 film, Dallas Buyers Club, ordering ISPs to hand over the account holder details of 4,726 IP address believed to be involved in infringing the film.[86] However, the court imposed several conditions on the rightsholders, designed to prevent speculative invoicing, a practice where rightsholders contact users with offers to settled alleged infringements for grossly disproportionate amounts.[87] The copyright owners were ultimately unwilling to comply with these conditions, and the account holder details were subsequently not provided to the copyright owners.[88]

Also in April 2015, a draft industry code developed by the Communications Alliance in consultation with ISPs, copyright owners and consumer representative groups was submitted to the Australian Communications and Media Authority (ACMA) for registration under the Telecommunications Act 1997 (Cth).[89] The draft code proposed a Copyright Notice Scheme that would have allowed copyright owners to send reports to ISPs identifying IP addresses alleged to have been used for copyright infringement. This would then have triggered obligations on the part of ISPs to send a series of escalating notices to subscribers about their alleged copyright

infringement. Although the draft code was submitted to the ACMA, it was not registered. The code was abandoned after ISPs and rightsholders could not reach agreement about who would bear the costs of the scheme.[90]

Additionally, rightsholders lobbied government to amend the law after the iiNet case, and in 2015 the Copyright Amendment (Online Infringement) Bill 2015 was passed, amending the Copyright Act 1968. This legislation introduced a website blocking regime which permits rights-holders to apply to the Federal Court for an order to have websites blocked by Telcos and ISPs if those websites are facilitating copyright infringement.[91] To obtain an order under the regime, the rightsholder must show that the website infringes, or facilitates an infringement of, copyright and that the primary purpose of the website is to infringe or facilitate copyright infringement.[92] If the order is made to block the website, the Telco or ISP must take all reasonable steps to disable access to the website.[93]

A concerning issue that arises with respect to the website blocking regime is the lack of transparency for website hosts and internet users. The only parties to any application under the website blocking regime are the rightsholder and the Telco/ISP. The person who operates the website may make an application to be joined to the proceeding, but has no right to be heard per se. Indeed, there is no requirement even to notify persons running a website that their website is the subject of an application. This effectively sets up a process which is inherently weighted in favour of blocking websites, because the process does not necessarily consider the opposing interests of the website host - what is not argued before the court may not be considered by the court.

Australian copyright law now includes laws that may permit authorities to require Telcos and ISPs to suspend or restrict access to websites, directly impacting on freedom of expression. There are very few requirements for public disclosure of requests made or actions taken for this purpose. Australia has exhibited a trend in law-making that affects Telcos and ISPs' ability to respect freedom of opinion and expression, through an unequal court process weighted in favour of website blocking. Telcos and ISPs are therefore operating in a legal environment where it may prove difficult to prevent, mitigate or challenge the human rights impact of Australian copyright law, particularly when these businesses are required to provide access to customer data.

Copyright law and the safe harbour regime

The copyright safe harbour scheme in Australia is deeply flawed, in that it only applies to

telecommunications providers, and not all internet intermediaries.[94]

Australia adopted the safe harbour regime as part of the 2005 Australia - US Free Trade Agreement (AUSFTA). The safe harbour regime was designed to provide a 'safe harbour' for internet intermediaries to protect them from copyright liability if they respond appropriately to complaints from copyright owners. Copyright owners can deliver a notice in the prescribed form alleging that content which the intermediary hosts is infringing copyright. The intermediary must then remove that material within a reasonable time in order to take advantage of the safe harbour. The system includes processes to ensure that the users who originally uploaded the allegedly infringing content are informed that the material has been removed and are provided with options to contest the complaint.

However, when legislation enacting the terms of AUSFTA was introduced in Australia, it contained a drafting error that limited its application only to 'Carriage Service Providers' (telecommunications providers and ISPs) but not to those entities who really need it - content hosts.

The lack of protection for most online intermediaries in Australia (including general content hosts, search engines, and social media platforms) creates a great deal of uncertainty and regulatory risk in Australian law.[95] Many foreign online services that allow users to upload content rely on the safe harbours to limit their legal risk. Without safe harbours, Australian technology entrepreneurs face greater legal risk than their competitors, and this contributes to a hostile environment that drives home-grown innovators offshore.

Further, without an effective notice and takedown scheme, Australian hosts have a strong incentive to remove speech in response to requests from third parties without a clear procedure for evaluating or contesting their validity. They may simply remove content on the fear of litigation, and they have no obligation to inform the uploading user that this action has been taken. The practical outcome is that the speech rights of Australian users are limited because intermediaries do not have the protection of a certain safe harbour scheme.[96]

The Australian Government has introduced a bill, the Copyright Amendment (Service Providers) Bill 2017, which purports to replace the term 'carriage service provider' in Australia's copyright safe harbours with, simply, 'service provider'.[97] This seems, on face value, like it would fix the drafting error that first occurred when Australia enacted the terms of AUSFTA. However, the Bill defines 'service provider' to be a carriage service provider; an organisation assisting persons with a disability; or a body administering a library, archives, cultural institution or educational institution.[98] While this would be an improvement on the current situation if passed into law, it still does not go far enough. It does not extend the safe harbour to Australia's internet hosts that actually need it.

Currently, because most Australian hosts are not covered by the safe harbours, there are no legal due process safeguards to protect either copyright owners or ordinary Australians who upload content to Australian digital services. In an age where major tech companies are responsible for making decisions that have real impact on freedom of speech for all internet users,[99] strong due process safeguards are important to protect legitimate businesses and the human rights of individuals.

Copyright law, access and fair use

A positive development that recently occurred in the copyright space was that the Australian Parliament passed the Copyright Amendment (Disability Access and other Measures) Act in June 2017.[100] The Act inserts new provisions into the Copyright Act 1968 to provide a new fair dealing exception for persons with access disabilities to permit them to copy books and other materials into formats that they can use, such as braille, large print, or audio.[101] The new amendments also provide protection to educational institutions and not-for-profit organisations who assist persons with access disabilities to make these copies.[102]

These amendments implement Australia's obligations under the Marrakesh Treaty,[103] which Australia signed in June 2014 and ratified in December 2015.[104] In fact, they go further than Australia's obligations, by extending the fair dealing beyond persons with visual or print disabilities. Amendments to the Copyright Act 1968 define 'person with a disability' as 'a person with a disability that causes the person difficulty in reading, viewing, hearing or comprehending copyright material in a particular form.'[105] This is an important advance by Australia's government.

Overall, the Copyright Amendment (Disability Access and other Measures) Act represents a major milestone in making copyrighted content more accessible. However, the Australian Government has still failed to respond to recommendations made by the Productivity Commission in 2016[106] and the Australian Law Reform Commission (ALRC) in 2014[107] that Australia adopt a broad, 'fair-use style' exception to copyright infringement.

A fair use exception would legalise many things that most people already consider legal, and would align with norms of reuse already evident in many creative communities.[108] It would allow creators to get on with being creators, without having to worry about trying to fit their creations into one of the narrow fair dealing exceptions or pay sometimes-exorbitant licensing fees in exchange for permission to use.[109] Critically, fair use would help to distinguish what the industry calls 'piracy' from acts that ordinary consumers do all the time and which don't harm creators.

Copyright law needs to be both simple and fair.[110] It needs to be a law that ordinary users can believe in. A fair use exception would help to restore copyright law's legitimacy and ensure that regular consumers and users are not treated like 'pirates'.

Recommendations:

The Australian Government should ensure that copyright laws are flexible, transparent and provide due process to users. This should include:

- **Proper due process and privacy safeguards included in the website blocking regime;**
- **Extension of the safe harbour provisions to all Australian online service providers; and**
- **A broad, general purpose, 'fair use style' exception to infringement to be included in the Copyright Act 1968 (Cth).**

Transparency in commercial content moderation

- A/Prof Nicolas Suzor

Telecommunications firms and internet companies play a major role in governing the material that users can share and view online. These providers are themselves subject to pressure from law enforcement agencies and private actors around the world to moderate content in different -- and sometimes conflicting -- ways. The decisions that these providers make are increasingly the subject of public interest, and a number of major controversies have erupted over the last decade as users try to understand and influence how content is moderated online.

Unfortunately, there is little good data available about how telecommunications providers and internet platforms make content moderation decisions. This leads to confusion among users and makes it more difficult to have an informed public debate about how to regulate internet content in a way that protects freedom of expression and other legitimate interests.

Recommendations:

Telecommunications providers and internet platforms must develop processes to increase transparency in content moderation by clearly explaining:

- **What content has been removed or triggered an account suspension.**
- **Who was responsible for making a decision to remove a user's content or suspend their account.**
- **Why a decision was made (including the specific rule that has been breached).**
- **How the moderation system was triggered, including a description of the role of algorithms, other users, law enforcement agencies, other third parties, and internal decision-makers in flagging, detecting, or evaluating prohibited content.**

In order to allow users to trust that content moderation systems are operating without bias and according to justifiable rules, this information must be provided at the level of individual removals and suspension as well as in an aggregate form.

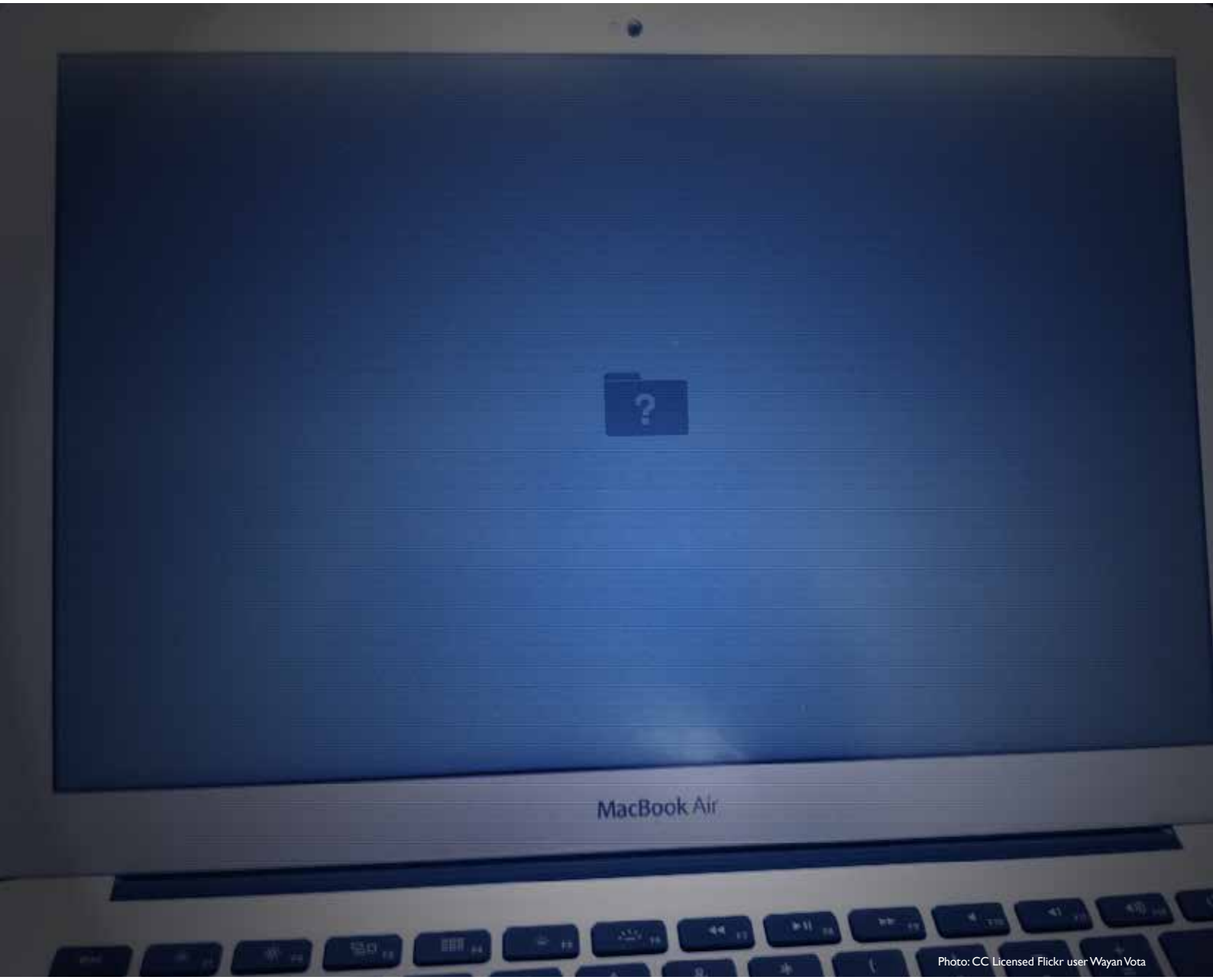


Photo: CC Licensed Flickr user Wayan Vota

Access to the internet as a human right

- Lizzie O'Shea

Australia still experiences a significant digital divide which impacts the human rights of a range of different social groups.

This trend was confirmed in the Digital Inclusion Index, which found problems among older Australians, indigenous people and people with disabilities, among others.[111] The Digital Inclusion Index, which aims to measure the level of digital inclusion across the Australian population, has proven to be a valuable tool to identify the problems with access to the internet and digital literacy. It will also hopefully impact policy proposals also over time.

The Australian government does have some initiatives that are underway to address this. It is currently in the process of rolling out the National Broadband Network (NBN), which is designed to address many of these problems. The purpose of the NBN is to 'deliver Australia's first national wholesale-only, open access broadband network to all Australians.'[112] This project is taking longer than expected, arising from strong differences of political opinion as to the technology choices to roll out the NBN.

It is worth noting that competition and consumer laws are arguably important to closing the digital divide. For example, a case brought by the Australian Competition and Consumer Commission against a mobile service provider was successful in obtaining damages and injunctive relief and penalties. The provider was found to have engaged in illegal behaviour, including representing to customers 'that mobile phone coverage was available at their home address when it was not, including to customers in remote indigenous communities where no coverage was available.'[113] These cases are necessary because the individual customers are likely to be vulnerable and will probably not have the means to bring a case themselves. Importantly, it shows that groups that do not have access to the internet are keen to find ways to address this. The Government must ensure that the industry is properly regulated to avoid telcos taking advantage of consumers who are seeking to gain access to the internet.

The Government must also ensure that access is guaranteed for those people with special needs, such as those who are blind, deaf or have other disabilities. Australia has adopted a number of both domestic and international instruments to promote inclusion of people with a disability. Australia has had a Commonwealth Disability Discrimination Act[114] in place since 1992 to protect the rights of Australians with a disability; and there is a 10 year National Disability Strategy[115] outlining how people with disability can be further included in Australian economic, social and community participation.

Whilst some of the work being undertaken through the building of the NBN, initiatives such as the National Year of Digital Inclusion in 2016, and the ACCC is intended to promote or enhance Internet accessibility and connectivity, there continue to be problems of access to much of Australia's networked society for people with a disability, such as cost, literacy and accessibility.

Photo: CC Licensed Nasa Goddard Space Flight Center

Children's rights in a digital age

- A/Prof Amanda Third

Australian children live, learn and grow up in a context of rapid technological change characterized by, among other trends, increasing mobile media penetration, and the rise of (visual) social media, user-generated content, new cultures of participation and consumption, artificial intelligence, and augmented and virtual reality.[116] As of June 2015, over 935,000 Australian teenagers (82%) reported having gone online in the previous month, an increase of 12% since 2011.[117] Girls in this age bracket are more likely to have been online than boys. Similarly, as of June 2013, 95% 8-11 year olds reported they had accessed the internet in the previous four weeks via a range of devices including desktop computers, laptops and mobile devices such as phones, tablets and games consoles.[118] The vast majority of Australian teenagers (86%) have broadband access at home. However, children and young people living in metropolitan centres are more likely to have access to the internet than their regional peers, pointing to a digital divide among children and young people. Children's and young people's most frequent point of access to the internet is from home, but they are also exposed to a range of digital platforms and services at school, at the homes of friends, and to a lesser degree via public internet connections.[119] Mobile phone connectivity is increasing rapidly, with Roy Morgan reporting in 2016 that nine out of ten Australian teenagers own a mobile phone, 94% of which have a smartphone.[120] Crucially, research shows that Australian children do not necessarily distinguish between the online and the offline worlds in the ways their adult counterparts often do.[121] Rather, they move flexibly across online and offline spaces, seeing digital spaces as just one other setting in which they live. Further, many young Australians see digital media as fundamental to their everyday lives.[122]

Given the fast pace of ongoing digital transformation, research, policy and practice internationally has frequently struggled to track and respond to the impacts of digital media use on a diverse array of children. It is commonly acknowledged that children's use of digital media exposes them to new forms of potential harm .[123] Children are frequently early adopters of digital media and their uptake sometimes outpaces that of their adult counterparts.[124] As a consequence, some children do not always benefit from appropriate levels of guidance and support from parents, caregivers, and educators .[125] Further, children are not always supported and protected by appropriate policy, legislative and regulatory mechanisms relating to 'the digital' .[126] In the face of such challenges, internationally, research, policy and practice relating to children's digital practices has focused primarily on mapping key uses, identifying the risks children encounter, and quantifying the harms they experience online .[127]

Importantly, not all Australian children are equally predisposed to the risks and potential harms. Nor are they all equally able to take advantage of the opportunities of being online. Research continues to show that those who are at risk offline are more at risk online, and our efforts need to identify and address these children more precisely.[128]

Amidst the concerns about children's online safety that dominate global research, policy and practice agendas, an

emerging body of research is demonstrating a range of benefits associated with children's online participation.[129] This research documents a wide range of potential positive outcomes, including impacts on children's formal and informal learning; health and wellbeing; literacy; civic and/or political participation; play and recreation; identity; belonging; peer, family and intergenerational relationships; individual and community resilience; and consumer practices.[130] Even so, a lack of rigorous data limits the capacity of policy and practice to promote the benefits of connectivity for children. Indeed, in a landmark report, Livingstone and Bulger identified that generating evidence about how to enable children to benefit from opportunities online is an urgent priority for the global research, policy and practice community.[131]

It is clear that protecting Australian children from harms online must remain a core component of research, policy and practice relating to children's digital media use.[132] At the same time, Australian children stand much to gain from their online engagements and efforts need to focus more systematically on enabling them to harness a broader range of opportunities online. As Gasser and Cortesi note in relation to the international scene, "recently, the previously predominately risk-oriented and issues-driven policy conversation has turned into a more holistic debate about the challenges and opportunities of digital technologies for children and their interests".[133] Even so, there is still much work to be done to translate the fruits of these conversations into concrete policy initiatives and practice outcomes for children in Australia. Thus, the key question confronting the Australian government, and NGOs and corporations operating in Australia is: How can we help children to better navigate risks online and foster their protection from harm online, whilst simultaneously empowering them to maximise the opportunities of connectivity? It is in this context that rights-based frameworks have begun to be embraced to guide effective policy and practice.

Children's rights are enshrined in the Convention on the Rights of the Child (UNCRC), which was adopted unanimously by the United Nations General Assembly in 1989. It has since become the most rapidly and widely ratified human rights treaty in history, and its operationalization is supported by a series of Optional Protocols and General Comments. The UNCRC encompasses a broader range of rights than any other human rights treaty, from humanitarian to economic, and socio-cultural to civil and political rights. While the UNCRC is not the first international treaty to protect children's rights,[134] it stands apart from previous declarations in that it grants children the right to express their opinion in matters that concern them, thus adding participation rights to those of protection and provision that were laid out by the UNCRC's precedents. Australia is a signatory to the UNCRC and is held accountable to the attendant duties and obligations to children by the UN's monitoring and reporting processes.

Children's digital rights have been an explicit concern of the international children's rights community since at least 2014 when, in observance of the 25th anniversary of both the adoption of the UNCRC and the release of

the code that would become the internet, the United Nations Committee for the Rights of the Child held a Day of General Discussion (DGD) on 'Digital Media and Children's Rights'. The DGD brought together global experts from across sectors to discuss how to interpret the UNCRC to harness the opportunities and meet the challenges of the digital age. It marked an attempt to seriously consider how to balance children's protection from harm online with promoting the benefits for children of their digital media engagement. Further, the DGD aimed to not only promote children's rights to access the internet safely but also to consider ways digital media might better enable children to understand and enact a broad range of rights in their everyday lives.

Within recent research, policy and practice, there are three ways children's rights are currently discussed in relation to digital media. The first focuses in on children's rights to digital media, which centres primarily around the problem of access. The second examines the extent to which children can enact their rights in online spaces. The third focuses more broadly on children's rights in the digital age, understanding connectivity as an increasingly fundamental condition of everyday life today and, in doing so, seeks to move beyond the artificial distinction between the online and offline worlds to think about how children's social and cultural digital practices might provide fertile terrain for advancing their rights both online and offline.[135] It is vital that Australian research, policy and practice continue to foreground these different dimensions of children's rights as they pertain to digital media.

Australia is uniquely positioned to play a key role in leading international debates and the development of interventions designed to guarantee children's rights. On the protection front, the 2015 legislation of the Office of the Children's eSafety Commissioner – which, while renamed as the Office of the eSafety Commissioner (The Office) in 2017, maintains children and young people's safe online engagement as a key mandate, while enabling an intergenerational focus to benefit children and young people – is the first agency internationally that is mandated to coordinating and leading the online safety efforts of government, industry and the not-for-profit community,[136] and has been a move that has been closely watched by the international online safety and child protection community. The Office provides a complaints service for young Australians who experience serious cyberbullying; identifies and removes illegal online content; and tackles image-based abuse. The Office also provides online safety educational content for Australian young people, women, teachers, parents, seniors and community groups.[137]

Additionally, the Office coordinates the Online Safety Consultative Working Group (OSCWG), expanded in 2017 to include a broad range of stakeholders from across community groups, internet service providers, industry associations, research organisations, business and government, to provide government with expert advice and guidance on measures to protect Australian children from online risks including cyber bullying, exposure to illegal content and privacy breaches.

The Office is committed to leveraging high quality evidence around issues relating to children's rights in the digital age. For example, in 2017, the Office hosted international child rights and digital media expert, Professor Sonia Livingstone (London School of Economics), and a range of Australian scholars with profile and interest in the promotion of children's and young people's rights in and through online spaces at an event to brainstorm how to better support children's online safety and the benefits of their digital engagements.

There is generally good coordination and information sharing across the youth and technology sector. In addition to the OSCWG, the Technology and Wellbeing Roundtable – auspiced by Telstra Corporation and ReachOut.com – has been meeting quarterly for over ten years to ensure good communication lines between different actors in the online safety, digital wellbeing, and digital youth engagement and participation spaces. This knowledge brokering entity has played a key role in agenda setting for policy and informally nurtured research, advocacy and service design and delivery partnerships around issues ranging from children's and young people's online safety and digital inclusion to their practices of digital citizenship, digital resilience and wellbeing.

The Australian Human Rights Commissioner, the National Children's Commissioner and UNICEF Australia have worked systematically over the last few years to surface and address the challenges of securing children's rights in the digital age, contributing to the creation of a setting in which Australian children's rights in the digital age can be effectively championed.

So too, Australia is home to a vibrant research community that is generating internationally renowned, cutting edge evidence and insights to guide policy and practice around children and young people's use of and participation and engagement via digital media (see for example the work of the Australian Communications and Media Authority, the Young and Well Cooperative Research Centre (2011-2016);[138] AU Kids Online;[139] the Parenting Research Centre's Raising Children Network;[140] and the cyberbullying research undertaken by the Centre for Child Health Promotion Research[141]). Some of this work, while internationally focused, has solicited the views of Australian children on their rights in the digital age.[142] Other Australian research was profiled in UNICEF's flagship publication, the 2017 State of the World's Children: Children in a Digital World report.[143] The National Children's Commissioner's Children's Rights Report 2015[144] report drew on a wide range of evidence to highlight some of the challenges pertaining to children's rights and digital media, particularly in relation to business. Importantly, this report also showcased Australian children's views on these issues, giving substance to Article 12 of the UNCRC, which stipulates that children have a right to participate in decision-making processes that impact their lives.

A number of Australian organisations deliver internationally respected, innovative education and services to children and young people via digital platforms (e.g. Project Rockit; ReachOut.com). Together, a broad range of Australian stakeholders has pushed the boundaries of thinking

about online safety, digital citizenship, digital inclusion, digital literacy, and digital resilience. In doing so, they have contributed significantly to the development of evidence-based, balanced debates, targeted education and programs, and policies and legislative protections for children.

Even so, there is still a long way to go to ensure the protection of children from harms associated with online participation, particularly of those children who are most vulnerable. Further, Australia is yet to best understand how to leverage digital technology to support children's and young people's education and learning, civic and political participation, health and wellbeing, and intergenerational relationships. Indeed, preparing children for the digital future, delivering on their rights to protection from harm, and promoting their opportunities online will require sustained attention and investment, particularly given that new technological developments such as artificial intelligence and machine learning, virtual reality, augmented reality, 3D printing and so on will bring with them new challenges and new opportunities for children's rights.

A recent Case for a General Comment on Children and Digital Media, commissioned by the Children's Commissioner of England, asserts that, internationally, states, NGOs, and corporates are calling for principled and evidence-based guidance to deliver on children's rights for the digital age.[145] A General Comment on Children and Digital media would support the provision of such guidance in the interpretation of the UNCRC, enabling duty bearers and implementing organisations to prioritise children's rights in relation to digital media. It is vital that the Australian government and vested community organisations and businesses provide their support to these efforts. In doing so, we can better guarantee the rights of Australian children, and contribute to the coordination of efforts to secure all children's rights, across national boundaries.

Recommendations:

Australian research, policy and practice must endeavour to minimise the potential harms and maximise the benefits of online engagement for Australian children, through the adoption of a child rights approach to governance, research and program delivery in relation to children's use of digital media.

A key goal of the policy and practice community must be to address all three dimensions of children's rights in relation to the digital world: a) children's access to digital media; b) their rights in online spaces, and how digital media can be harnessed to deliver on a broad range of children's rights.

The Australian government, NGOs, corporations and research organisations should actively engage children and young people in developing responses that protect their rights to provision, protection and participation in the digital age, and develop child-centred measures of impact.

The rights of disadvantaged children must be centred more consistently across Australian research, policy and practice interventions.

Investment should be channelled into research that examines both the potential harms and the benefits of children's digital media use.

The Australian government should continue to support the eSafety Commissioner's Office and find further mechanisms to support cross-sector knowledge sharing; ongoing research; policy development; and evidence-based programmatic responses to support children's rights in the digital age.

The Australian government should lend support to the Case for a General Comment on Children and Digital Media to guide states, NGOs and corporations in their interpretation of the Convention on the Rights of the Child for the digital age.

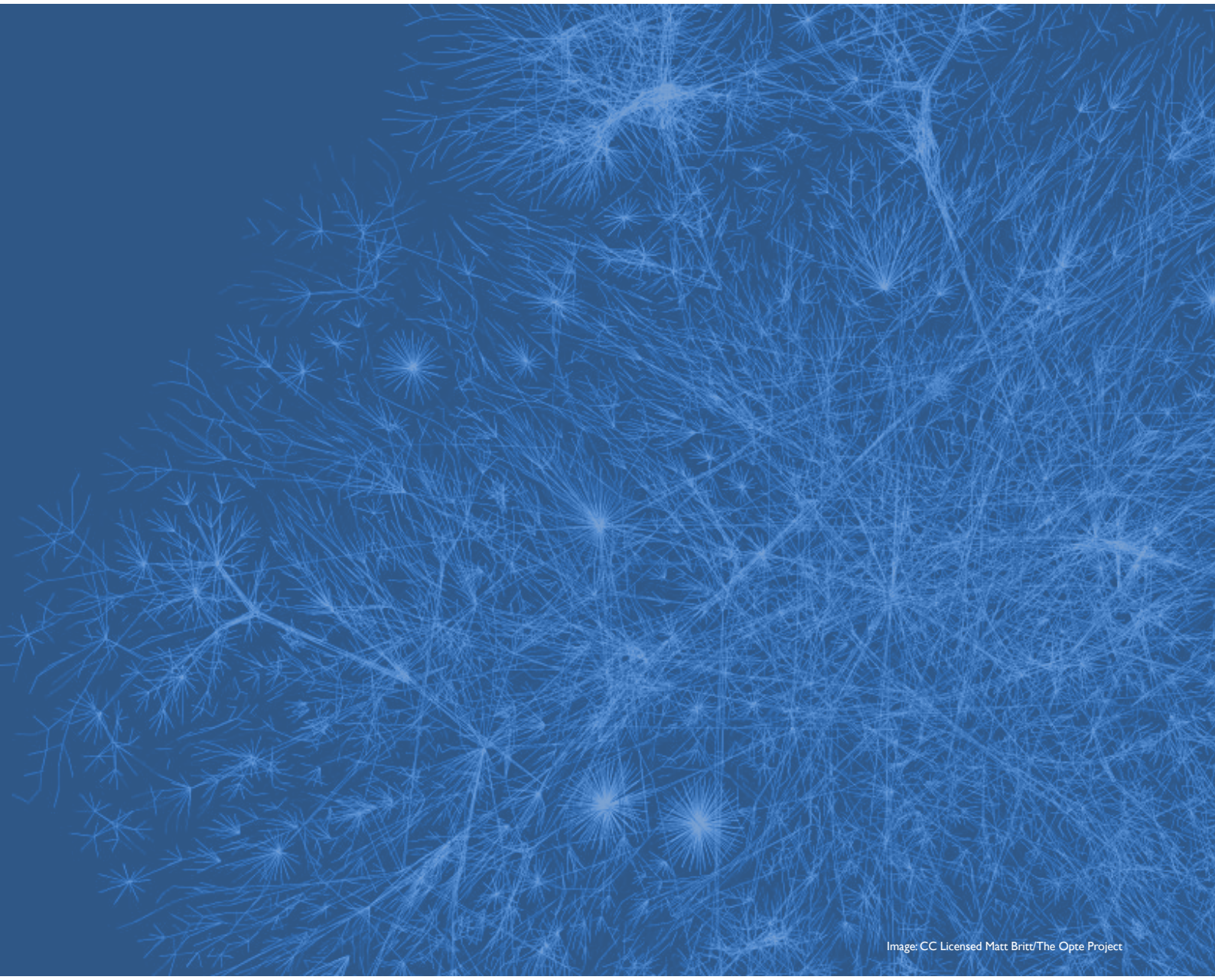


Image: CC Licensed Matt Britt/The Opte Project

Appendix: Public perceptions of digital rights

Australians are some of the world's greatest users of social media and mobile broadband, and our nation is in the top ten globally for internet use. At a time when our use of these technologies is increasingly redefining aspects of our personal and professional lives, the University of Sydney report *Digital Rights in Australia*[146] explores urgent questions about the nature of our rights now and into the future.

The analysis covers rights issues in four areas: privacy, profiling and analytics; government data matching and surveillance; workplace change; and freedom of expression and speech regulation.

In developing their report, researchers undertook a national survey of the attitudes and opinions of 1600 Australians on key rights issues; focus group discussion of related rights scenarios; and an analysis of legal, policy and governance issues.

Their core findings are re-published here, with permission.

Privacy, Profiling, Data Analytics

Australians are concerned about their online privacy. While two thirds of respondents believe they personally have nothing to hide, only a small group (18%) think that more general concerns about online privacy are exaggerated.

A majority of respondents do not feel in control of their privacy online. While a majority take active steps to protect their privacy (67%), and have changed settings on the social media they use most often (61%), a minority (38%) felt that they can control their privacy online.

Women experience the online world differently from men: they are more likely to agree that they actively protect their privacy online (71%, compared with 63% of men) and change their social media settings (63%, compared with 58% of men), but feel no more in control of their privacy (39%, compared with 38% of men).

There may be a significant group for whom the answer to questions relating to privacy online are: "it depends" (this contrasts with answers about governments and privacy).

Corporations were the major source of concern: 57% were concerned about their privacy being

violated by corporations, although a substantial number were also concerned about privacy violations by government (47%) and other people (47%).

A large majority (78%) want to know what social media companies do with their personal data.

Government Data Matching and Surveillance

Nearly half of respondents were concerned about government violating their privacy (47%).

A majority is opposed to government programs for phone companies and internet service providers to keep metadata on phone calls and web use. 79% of respondents considered retention of information about phone calls to be a privacy breach. A majority (58%) were also opposed to a policy for government- mandated retention of information about internet communications.

But a change in frame altered these numbers. When asked whether they favour law enforcement and security agencies being able to access metadata, the number in favour jumped up to 42% (47% opposed). Once framed as an anti-terrorism measure, government data-gathering about internet is supported by a majority of respondents (57%), while only 31% oppose a program described this way.

Respondents' attitudes towards both government collection of communications data, and government data matching programs, varied significantly depending on political identification. Respondents who identified with the Coalition were significantly more likely to support programs; identification with the Greens made a respondent more likely to oppose such programs.

There is considerable ambivalence among the survey participants towards online government data matching programs. We found that 42% are in favour and 45% are opposed to a program that tracks people's use of public services and benefits.

Work

Digital privacy at work matters. Most Australians do not think employers should look at their employees' social media pages. While 37% agreed that it was acceptable for either prospective or current employers to look at public social media posts; only 20% agreed that it was ok for either current or prospective employers to look at private posts.

High school educated, those not working in professional/skilled work, and respondents over 40, were most concerned about employers accessing their social media posts.

Only 16% of people agreed that using social media was an important part of their job, but most workplaces (72%) they were in had a policy about using social media while at work. Most workplaces seem to recognize the everyday ubiquity of social media use and are attempting to govern it, though only 46% of respondents said their workplace had a policy on what they post online.

In this terrain of unclear directions over social media at work and employers' rights to access posts, our online discussion groups reinforced that privacy boundaries are important, but also that employees needed to use their own "common sense".

The encroachment of some new policy agendas, such as that seen in the case study of the Public Service Commission, needs to better reflect people's desires for digital privacy at, and from, work.

The app driven, online gig economy presents a new space for digital rights analysis. Most respondents have heard of, but not used, a platform such as Uber, Airtasker or Deliveroo; and use is skewed towards those under 40 and the university educated.

Australians see gig work as providing workers with more flexibility, but at the same time a majority are also concerned about the financial insecurity of this kind of work. Over 60% believe that these new forms of work need new government regulations.

Speech

Australians are not strongly wedded to the North American ideal of absolute speech freedom online. Just over a third (37%) of those surveyed agreed that

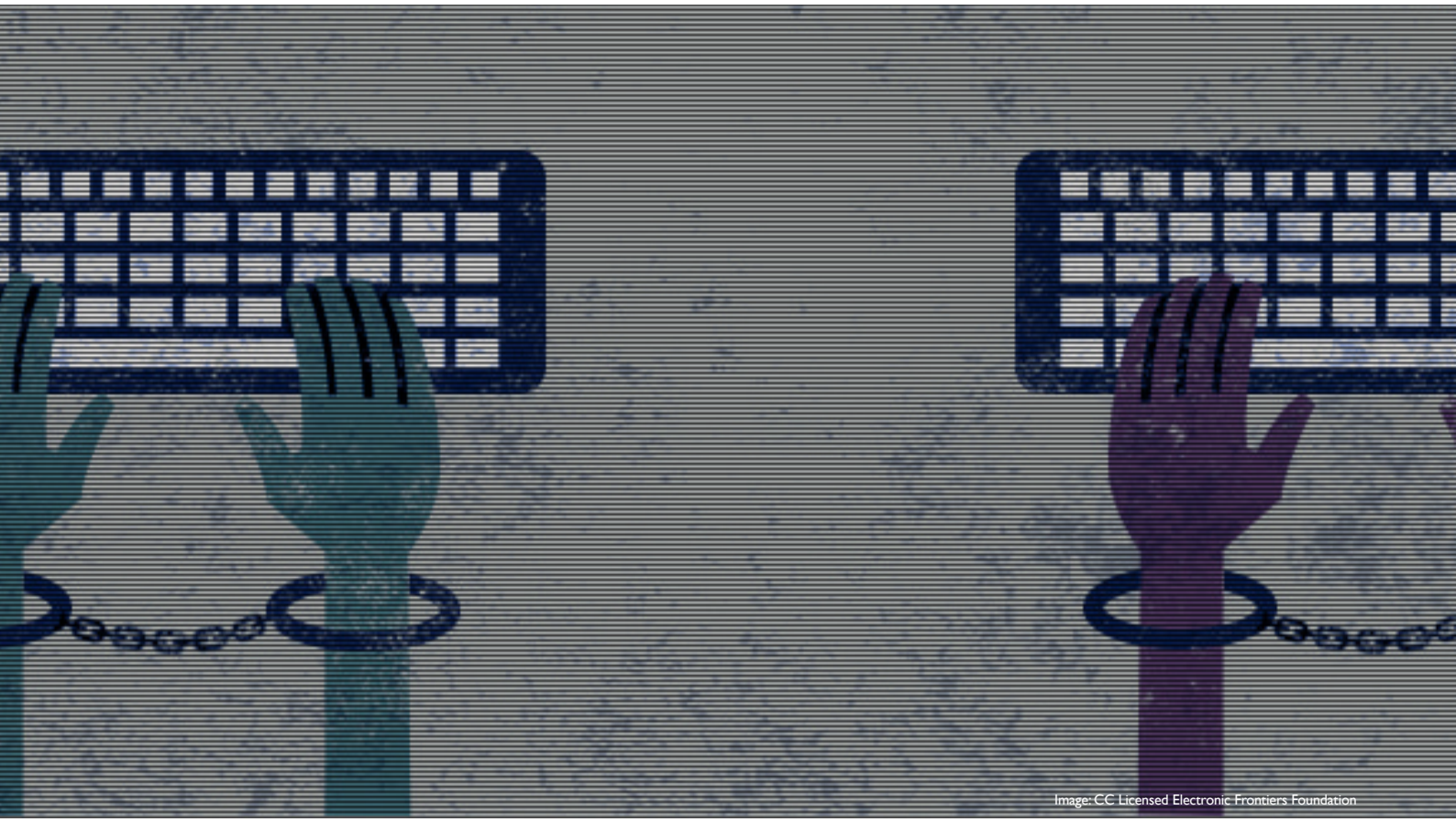


Image: CC Licensed Electronic Frontiers Foundation

they should "be free to say and do what I want online", but 30% disagreed and a third expressed reservations about the idea. People were also less supportive of others having that absolute freedom than themselves.

50% of Australians agreed that everyone should have the right to online anonymity or pseudonymity, a figure that increases to 57% for those under 40 years. Around a third of younger Australians said it was more likely that they would make honest and open comment on the news, talk about sensitive topics like sexuality or question others' opinions if they had the opportunity to comment anonymously.

Men are more likely to assert their right to free expression than women, reflecting the male dominance of everyday speech online as much as offline.

Gender is a key variable in understanding attitudes to social media regulation. Men were less likely than women to agree with the need to remove within 24 hours instances of sexual harassment, abuse targeted at an individual, or hate speech that encourages violence against others. Women were less supportive than men of the right to anonymity.

While most Australians had not experienced negative impacts from risky or harmful online speech, 39% have been affected by mean or abusive remarks and 27% have had personal content posted without consent.

More than was the case for either work or privacy issues, Australians agreed on the need for more regulation of online discussion environments. They flagged the need for increased involvement by social media platforms in content moderation and 'easy' complaints reporting.

There was a perception gap between people's belief that harmful social media content was easy to get taken down, and the procedural reality that it is not always straightforward and may require regulatory intervention to persuade the host company to act.

Endnotes

1 The relevant bill amended the Telecommunications (Interception and Access) Act 1979 and received Royal Assent on 13 April 2015. The specific metadata that must be retained is set out in a list in the statute.

2 See comments of Edward Snowden, Oliver Milman, "Edward Snowden says Australia's new data retention laws are dangerous," The Guardian, 9 May 2015 https://www.theguardian.com/us-news/2015/may/09/edward-snowden-saysaustralias-new-data-retention-laws-are-dangerous.

3 Mark Colvin, "AFP admits AFP admits extreme surveillance on reporter, setting off media freedom row", ABC radio, 16 April 2017, http://www.abc.net.au/ pm/content/2016/s4443273.htm; Christopher Knaus, 'Federal police admit to accessing journalist's metadata without a warrant,' The Guardian, 28 April 2017 https://www.theguardian.com/australia-news/2017/apr/28/federal-policeadmit-accessing-journalists-metadata-without-a-warrant.

4 Tele2 Sverige AB v Post-och telestyrelsen; Secretary of State for the Home Department v Watson and others (C-203/15 and C-698/15), EU:C:2016:970, [108].

5 See for example Daniel Hurst, 'Mandatory metadata retention becomes law as Coalition and Labor combine,' The Guardian 26 March 2015; https://www.theguardian. com/australia-news/2015/mar/26/mandatory-data-retention-becomes-law-ascoalition-and-labor-combine; GetUp! 'Go dark against data retention,' https:// www.getup.org.au/campaigns/digital-freedom-and-privacy/go-dark-against-dataretention/go-dark-against-data-retention; Ros Page, 'Data retention regime now in effect,' Choice, 26 April 2017 https://www.choice.com.au/electronics-and-technology/ internet/internet-privacy-and-safety/articles/mandatory-data-retention-regime-onits-way; Will Ockenden, Metadata retention scheme deadline arrives, digital rights advocates say 'get a VPN', 'ABC News, 13 April 2017 http://www.abc.net.au/news/2017- 04-13/metadata-retention-scheme-deadline-arrives/8443168.

6 Nicolas P Suzor, Kylie M Pappalardo and Natalie McIntosh, 'The Passage of Australia's Data Retention Regime: National Security, Human Rights, and Media Scrutiny' (2017) 6(1) Internet Policy Review <https://policyreview.info/articles/analysis/passage-australias-data-retention-regime-national-security-human-rights-and-media>.

7 Benjamin Sveen, 'Data Retention Bill: Government departments ask AFP to access metadata after legislation enacted,' ABC, 3 October 2016 http://www.abc.net.au/ news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648.

8 ICCPR article 19 and article 17

9 [2017] FCAFC 4 .

10 Telstra Corporation Limited and Privacy Commissioner [2015] AATA 991 at [116].

11 Ben Grubb and Telstra Corporation Limited [2015] AICmr 35 at [171] - [172].

12 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at [5].

13 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at [73].

14 The Information Commissioner of Canada v The Executive Director of the Canadian Transportation Accident Investigation and Safety Board and NAV Canada [2007] 1 FCR 203; 2006 FCA 157.

15 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at [77].

16 Privacy Commissioner v Telstra Corporation Limited [2017] FCAFC 4 at [78].

17 Article 19 of the Universal Declaration of Human Rights 1948 (UDHR), Article 19 of the International Covenant on Civil and Political Rights 1966 (ICCPR), Theme 2 of the Association for Progressive Communications (APC) Internet Rights Charter 2001 at https://www.apc.org/en/node/5677 (APC Charter).

18 Article 20 UDHR, Article 20 ICCPR.

19 Article 27 UDHR, and Articles 1.1, 3 and 15(a) of the International Covenant on Economic, Social and Cultural Rights 1966 (ICESC), Themes 3 and 4 of the APC Charter

20 Article 1.1, ICCPR and Article 1.1 ICESC.

21 Articles 2 and 7, UDHR, Articles 4, 24 and 26, ICCPR.

22 Article 12 of the UDHR, Article 17 of the ICCPR, Theme 5 of APC Charter, and see too the International Principles on the Application of Human Rights to Communications Surveillance 2014 (also known as "Necessary and Proportionate") (May 2014) at http://necessaryandproportionate.org/principles

23 Article 13, UDHR.

24 As the US Federal Trade Commission noted, "use of big data analytics to make predictions may exclude certain populations from the benefits society and markets have to offer" - US Federal Trade Commission, Big Data: A tool for inclusion or exclusion? January 2016, p 9, accessed at: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf, pages 8 and 9.

25 Article 12, UNHR, Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (Report 123, 2014), https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123, Recommendations (unnumbered page towards the front of the report)

26 Articles 2(3) and 17 of the ICCPR.

27 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (Report 123, 2014), https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123, Recommendations (unnumbered page towards the front of the report)

28 Association for Progressive Communications, https://www.apc.org/en/pubs/about-apc/apc-internet-rights-charter.

29 George Williams and Daniel Reynolds, A Charter of Rights for Australia, UNSW Press, Sydney, 2017, p 37.

30 The Act applies to most Australian and Norfolk Island Government agencies, all private sector and not-for-profit organisations with an annual turnover of more than $3 million, all private health service providers and some small businesses– see https://www.oaic.gov.au/agencies-and-organisations/business-resources/privacy-business-resource-10.

31 Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSWLawJl 6; (2017) 40(1) University of New South Wales Law Journal 121, at 122.

32 The States have their own legislation. Relevant Commonwealth legislation includes: Part 5-1A of the Telecommunications (Interception and Access) Act 1979 ('TIA Act') (relating to data retention obligations), the Telecommunications Act 1997, the Intelligence Services Act 2001, the Surveillance Devices Act 2004 and the Australian Federal Police Act 1979 (Cth), s 60A(2) of which allows federal police recording and retaining of personal information. The AFP is legally permitted to collect facial images where it is 'reasonably necessary to fulfil its policing functions' and share them when it is 'reasonably necessary for law enforcement purposes' Attorney-General's Department (Cth), 'Face Matching Services' (Fact Sheet) 3 <https://www.ag.gov.au/ RightsAndProtections/IdentitySecurity/ Documents/Fact-Sheet-National-Facial-Biometric-Matching- Capability.pdf>.

33 Not covered are: the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Australian Signals Directorate, the Defence Intelligence Organisation, the Australian Geospatial-Intelligence Organisation. Office of the Australian Information Commissioner, "Which law enforcement agencies are covered by the Privacy Act?" at https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement.

34 Office of the Australian Information Commissioner, "Which law enforcement agencies are covered by the Privacy Act?" at https://www.oaic.gov.au/individuals/faqs-for-individuals/law-enforcement-surveillance-photos/resources-on-law-enforcement. It should be noted that the Australian Government Agencies Privacy Code (available at https://www.oaic.gov.au/privacy-law/privacy-registers/privacy-codes/privacy-australian-government-agencies-governance-app-code-2017) was registered on 27 October 2017 and comes into effect on 1 July 2018. It is a relatively short document which sets out specific requirements for government agencies to which the Privacy Act applies to assist them in adopting a best practice approach to privacy governance.

35 Privacy and Personal Information Protection Act 1998 (NSW); Information Privacy Act 2009 (Qld); Premier and Cabinet Circular No 12 (SA); Personal Information Protection Act 2004 (Tas); Information Privacy Act 2000 (Vic); Information Privacy Act 2014 (ACT); Information Act (NT).

36 Under s 62 of the Privacy and Personal Information Protection Act 1998 (NSW) the unauthorised or corrupt use or disclosure by a public official of personal information obtained through their official functions is an offence punishable by up to 100 penalty units or imprisonment for up to two years.

37 Monique Mann and Marcus Smith, "Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight" [2017] UNSW Law JI 6; (2017) 40(1) University of New South Wales Law Journal 121, at 123 and 125, in the context of facial recognition.

38 Sections 36, 40, 52.

39 Australian Law Reform Commission, Serious Invasions of Privacy in the Digital Era (Report 123, 2014), https://www.alrc.gov.au/publications/serious-invasions-privacy-digital-era-alrc-report-123, par 1.17.

40 Val Morgan DART 2.0 advertisement https://youtu.be/dj-mvoSucHY

41 Cadmus online assessment tool

42 Privacy Act 1988 https://www.legislation.gov.au/Details/C2017C00283/ Download Also available at the Office of the Australian Information Commissioner website: https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles#australian-privacy-principle-2-anonymity-and-pseudonymity

43 Behavioural biometrics – the future of security. By Jamie Carter, September 09, 2015, Techradar. Some major players are showing an interest in behavioural biometrics. http://www.techradar.com/news/world-of-tech/future-tech/behavioural-biometrics-the-future-of-security-1302888

44 Digital identity fraud protection. Infused with layers of cognitive fraud detection and analytics, IBM Trusteer helps you identify the difference between customers and fraudsters. And with greater accuracy, you won't waste time chasing false positives. https://www.ibm.com/security/campaign/trusteer-fraud-detection.html

45 UNDERSTANDING THE MATHS IS CRUCIAL FOR PROTECTING PRIVACY, Publishing data can bring benefits, but it also can be a great risk to privacy. By Dr Chris Culnane, Dr Benjamin Rubinstein and Dr Vanessa Teague, Department of Computing and Information Systems, University of Melbourne. https://pursuit.unimelb.edu.au/articles/understanding-the-maths-is-crucial-for-protecting-privacy

46 Westpac testing AI to monitor staff and customers, Australian Financial Review by James Eyers. http://www.afr.com/technology/westpac-testing-ai-to-monitor-staff-and-customers-20171113-gzks7h#ixzz4yvH2Tf6r

47 Computer vision and emotional privacy. University of Oxford, Practical Ethics. By Hannah Maslen. http://blog.practicalethics.ox.ac.uk/2014/03/computer-vision-and-emotional-privacy/

48 The new way university cheats are being caught. The Sydney Morning Herald. By Henrietta Cook. http://www.smh.com.au/national/the-new-way-university-cheats-are-being-caught-20160818-gqvuwg.html

49 University abandons Cadmus anti-cheating software. The software would have registered students' locations when writing essays on the app. by Zoe Stojanovic-Hill. http://honisoit.com/2017/07/university-abandons-cadmus-anti-cheating-software/

50 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression , Frank La Rue. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

51 Office of the Australian Information Commissioner (OAIC) - Privacy regulatory action policy. https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/

52 The UKUSA Agreement is not public, although request for it are pending in a case before the European Court of Human Rights, however, it is believed to be an annex of the British US Communications Intelligence Agreement and Outline of 5 March 1946, drafts of which were made public in 2010 https://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf

53 Lander, S. (2009) "International intelligence cooperation: an inside perspective" in Aldrich, R. J., et al. (2009). Secret intelligence : a reader. London, Routledge., p. 145

54 Richelson, J. and D. Ball (1985). The ties that bind : intelligence cooperation between the UKUSA countries - the United Kingdom, the United States of America, Canada, Australia and New Zealand. Sydney: George Allen & Unwin. p. 301

55 ibid p. 301

56 Hager, N (1996) Secret Power: New Zealand's Role in the International Spy Network Craig Potton, Nelson, New Zealand, http://www.nickyhager.info/Secret_Power.pdf p.45

57 Warner, M. (2014) The Rise and Fall of Intelligence an international

security history Washington: Georgetown University Press,. Available at: http://ezproxy.library.usyd.edu.au/login?url=http://www.jstor.org/stable/10.2307/j.ctt6wpkvt Online text. p.143

58 Ball, D. (1980). A suitable piece of real estate : American installations in Australia. Sydney, Hale & Iremonger. p 15

59 Senate Question Time Monday 22 February 2016, Hansard p. 50 http://parlinfo.aph.gov.au/parlInfo/download/chamber/hansards/3efbd6eb-f185-4321-93ce-26b4047c1700/toc_pdf/Senate_2016_02_22_4097.pdf;fileType=application%2Fpdf#search=%22chamber/hansards/3efbd6eb-f185-4321-93ce-26b4047c1700/0000%22

60 Ben Eltham, 27 May 2015, Terror at Home, Overland Literary Journal, https://overland.org.au/2015/05/terror-at-home/

61 The New Zealand Government Communications Security Bureau has been given increased powers of surveillance in the Countering Terrorist Fighters Legislation. In Canada, Bill C-51 grants spy agency extra powers including to operate overseas for the first time. In addition, the Protecting Canadians from Online Crime Act was rushed through the parliament, providing immunity from civil liability for service providers disclosing data to law enforcement voluntarily and without a warrant. Without debate permitted, the UK government pushed the Data Retention and Investigatory Powers Bill (DRIP) through the parliament in 2014, reinstituting data retention measures the European Court found to be illegal, compelling companies outside the UK to execute a UK interception warrant and legalizing UK government access to submarine cables that don't go through the UK or its territorial waters. The USA Freedom Bill, while the first action in the US Congress that diminishes rather than expands surveillance powers, has been criticised as inadequate and largely symbolic because it does not alter the NSA's power to scan internet traffic in and out of the US or restrict in any way its spying on non-US citizens.

62 Google, Yahoo, Facebook, WhatsApp and Apple all sought to ensure clients of efforts to enhance security and end-to-end encryption of their social media products and email services, with Facebook making their site https by default.

63 HAYDEN MOCKS EXTENT OF POST-SNOWDEN REFORM: "AND THIS IS IT AFTER TWO YEARS? COOL!", The Intercept, June 18 2015 https://firstlook.org/theintercept/2015/06/17/hayden-mocks-extent-post-snowden-surveillance-reform-2-years-cool/

64 Edward Snowden: The World Says No to Surveillance, New York Times, June 4, 2015 http://www.nytimes.com/2015/06/05/opinion/edward-snowden-the-world-says-no-to-surveillance.html

65 Herman, M. (2004). "Ethics and Intelligence after September 2001." Intelligence and National Security 19(2): 342-358. p.356

66 Walsh, P. F. and S. Miller (2015). "Rethinking 'Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden." Intelligence and National Security: p.4

67 Horner, D. M. The spy catchers : the official history of ASIO, 1949-1963

68 UK Investigatory Powers Act 2016 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

69 UK's new Snoopers' Charter just passed an encryption backdoor law by the backdoor, The Register, 30 Nov 2016, https://www.theregister.co.uk/2016/11/30/investigatory_powers_act_backdoors/

70 How the Turnbull government plans to access encrypted messages , Sydney Morning Herald, 11 June 2017, http://www.smh.com.au/federal-politics/political-news/how-the-turnbull-government-plans-to-access-encrypted-messages-20170609-gwoge0.html

71 WHAT KIND OF REAR WINDOW INTO ENCRYPTION DO THE FIVE EYES WANT? Pursuit, Melbourne University, 2 July 2017, https://pursuit.unimelb.edu.au/articles/what-kind-of-rear-window-into-encryption-do-the-five-eyes-want

72 Thousands of Australians hit by private health insurance data breach, SBS, 17 July 2017, http://www.sbs.com.au/news/article/2017/07/17/thousands-australians-hit-private-health-insurance-data-breach

73 Australia's plan to force tech giants to give up encrypted messages may not add up , The Guardian, 14 July 2017, https://www.theguardian.com/technology/2017/jul/14/forcing-facebook-google-to-give-police-access-to-encrypted-messages-doesnt-add-up

74 Police want to read encrypted messages, but they already have significant power to access our data, Australian Privacy Foundation, 9 Sept 2017, https://www.privacy.org.au/2017/09/09/police-want-to-read-encrypted-messages-but-they-already-have-significant-power-to-access-our-data/

75 The Digital Economy: Opening up the conversation, Australian Government, Sept 2017, https://industry.gov.au/innovation/Digital-Economy/Documents/Digital-Economy-Strategy-Consultation-Paper.pdf

76 Australia's Cyber Security Strategy, Australian Government, April 2016, https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf

77 Australia's International Cyber Engagement Strategy, Australian Government, October 2017, http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/preliminary_information/introduction.html

78 B, C and D v Australian Postal Corporation T/A Australia Post [2013] FWCFB 6191

79 Gmitrovic v Australian Government, Department of Defence (2014) FWC 1637

80 Daniel Starr v Department of Human Services [2016] FWC 1460

81 Escape Hair Design (2010) 204 IR 292; [2010] FWA 7358

82 The right to disconnect', (2017), Bersay Associates http://www.bersay-associes.com/en/2017-01/the-right-to-disconnect/

83 Mann, M. and Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and southern criminology. In K. Carrington, R. Hogg, J. Scott and M. Sozzo (Eds.) The Palgrave Handbook of Criminology and the Global South (pp. 245-260), Springer: Cham, Switzerland; Mann, M., Warren, I. and Kennedy, S. (2018). The legal geographies of transnational cyber-prosecutions: Extradition, human rights and forum shifting. Global Crime, online first; Molnar, A., Parsons, C., & Zouave, E. (2017). Computer network operations and 'rule-with-law' in Australia. Internet Policy Review, 6(1), 1-14. doi: 10.14763/2017.1.453; Warren, I. (2015). Surveillance, criminal law and sovereignty. Surveillance and Society 13(2), 300-305; Molnar, A., 2017. Technology, Law, and the Formation of (II) Liberal Democracy?. Surveillance & Society, 15(3/4), p.381.

84 Roadshow Films Pty Ltd v iiNet Ltd [2012] HCA 16 (20 April 2012); 248 CLR 42. http://eresources.hcourt.gov.au/showCase/2012/HCA/16.

85 See Suzor, Nicolas P., Choi, Rachel, & Pappalardo, Kylie M. (2016)

Moments of flux in intermediary liability for copyright infringement. In Perry, Mark (Ed.) Intellectual Property Governance for the 21st Century: Global Evolution. Springer, pp. 129-149.

86 Dallas Buyers Club LLC v iiNet Ltd [2015] FCA 317 (7 April 2015).

87 See Pappalardo, Kylie M. & Brough, Carrick (2017) Dead cats in the mail: Dallas Buyers Club and the emergence of the user in Australian intermediary copyright law. In Gilchrist, John Steel & Fitzgerald, Brian F. (Eds.) Copyright, Property and the Social Contract. Springer.

88 See Allie Coyne, 'DBC gives up on iiNet piracy case,' IT News, 10 February 2016 http://www.itnews.com.au/news/dbc-gives-up-on-iinet-piracy-case-414920 ('Perram had set a $600,000 bond as a condition of his lifting the stay of the April 2015 preliminary discovery order, which gave DBC LLC access to the account holder details on a conditional basis….He ruled DBC LLC had failed to address his concerns about going after account holders for high damages.')

89 Communications Alliance Ltd, C653:2015– Copyright Notice Scheme Industry Code, http://www.commsalliance.com.au/__data/assets/pdf_file/0005/48551/C653-Copyright-Notice-Scheme-Industry-Code-FINAL.pdf.

90 Renai LeMay, 'Internet piracy code stalls on costs', Delimiter, 22 July 2015, http://delimiter.com.au/2015/07/22/internet-piracy-code-stalls-on-costs/; Allie Coyne, 'ISPs blindsided by 'shelved' Australian piracy code,' IT News, 18 February 2016 http://www.itnews.com.au/news/isps-blindsided-by-shelved-australian-piracy-code-415324.

91 Copyright Act 1968 (Cth), s. 115A.

92 Copyright Act 1968 (Cth), s. 115A(1).

93 Copyright Act 1968 (Cth), s. 115A(2).

94 Peter Leonard, 'Safe Harbors in Choppy Waters-Building a Sensible Approach to Liability of Internet Intermediaries in Australia' (2010) 3 J. Int'l Media & Ent. L. 221.

95 Rebecca Giblin, 'The uncertainties, baby: Hidden perils of Australia's authorisation law' (2009) 20 Australian Intellectual Property Journal 148

96 See generally 'Manila Principles on Intermediary Liability' (2015) https://www.manilaprinciples.org

97 Copyright Amendment (Service Providers) Bill 2017, introduced to the Senate on 6 December 2017, https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1115.

98 Copyright Amendment (Service Providers) Bill 2017, Schedule 1, s6.

99 See David Kaye, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (A/HRC/32/38, United Nations, Human Rights Council, 11 May 2016) http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Privatesectorinthedigitalage.aspx

100 Copyright Amendment (Disability Access and Other Measures) Bill 2017 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5832.

101 Copyright Amendment (Disability Access and Other Measures) Act 2017 (Cth), Sch. 1, s. 2 inserts a new s113E (Fair dealing for purpose of access by persons with a disability) into the Copyright Act 1968 (Cth).

102 Copyright Amendment (Disability Access and Other Measures) Act 2017 (Cth), Sch. 1, s. 2 inserts a new s113F (Use of copyright material by organisations assisting persons with a disability) into the Copyright Act 1968 (Cth).

103 Marrakesh Treaty to Facilitate Access to Published Works for Persons who are Blind, Visually Impaired or Otherwise Print Disabled, http://www.wipo.int/treaties/en/ip/marrakesh.

104 http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=843.

105 Copyright Act 1968 (Cth), s 10(1).

106 Productivity Commission, Intellectual Property Arrangements, Final Report, 20 December 2016, http://www.pc.gov.au/inquiries/completed/intellectual-property#report.

107 Australian Law Reform Commission, Copyright and the Digital Economy (ALRC Report 122), 13 February 2014, https://www.alrc.gov.au/publications/copyright-report-122.

108 Kylie Pappalardo and Karnika Bansal, 'How copyright law is holding law is holding back Australian creators', The Conversation, 9 February 2018, https://theconversation.com/how-copyright-law-is-holding-back-australian-creators-91390.

109 Ibid.

110 Nicolas Suzor, 'The only way to fix copyright is to make it fair', The Conversation, 21 February 2014, https://theconversation.com/the-only-way-to-fix-copyright-is-to-make-it-fair-23402.

111 Julian Thomas, Josephine Barraket et al, Measuring Australia's Digital Divide: The Australian Digital Inclusion Index 2016, p 5

112 See NBN, Our Purpose, http://www.nbnco.com.au/corporate-information/about-nbn-co/our-purpose.html .

113 Australian Competition and Consumer Commission, 'Court finds Excite Mobile acted unconscionably,' 22 April 2013, https://www.accc.gov.au/media-release/court-finds-excite-mobile-acted-unconscionably .

114 Disability Discrimination Act 1992 https://www.comlaw.gov.au/Series/C2004A04426

115 Department of Social Services https://www.dss.gov.au/our-responsibilities/disability-and-carers/program-services/government-international/nationaldisability-strategy

116 In accordance with the definition used by United Nations Convention on the Rights of the Child and UNICEF, children are defined here as those under the age of eighteen.

117 Research snapshots: Aussie teens and kids online, ACMA https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Aussie-teens-and-kids-online

118 Kids online: The statistics , Kidsmatter, https://www.kidsmatter.edu.au/health-and-community/enewsletter/kids-online-statistics

119 Research snapshots: Aussie teens and kids online, ACMA https://www.acma.gov.au/theACMA/engage-blogs/engage-blogs/Research-snapshots/Aussie-teens-and-kids-online

120 9 in 10 Aussie teens now have a mobile , Roy Morgan, August 2016, http://www.roymorgan.com/findings/6929-australian-teenagers-and-their-mobile-phones-june-2016-201608220922

121 Black, R. & Walsh, L. 2011. 'Students in the lead: increasing participation by young people in a distributed leadership framework'. In Mackay,

Tony and Zbar,Vic (ed), Leading the education debate: selected papers from the CSE series and occasional papers, 2007-2010, Centre for Strategic Education, East Melbourne,Vic., pp.240-251; Richardson, I, Third, A. & McColl, I. 2007. 'Moblogging and Belonging: New Mobile Phone Practices and Young People's Sense of Social Inclusion', DIMEA 2007: Second International Conference on Digital Interactive Media in Entertainment and Arts.Perth, Murdoch University, pp. 73-78.

122 Third, A et al. 2014. Children's rights in the digital age: A download from children around the world. Young and Well CRC/UNICEF. https://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf

123 Livingstone, S. and Bulger, M. 2013. A Global Agenda for Children's Rights in the Digital Age. Florence: UNICEF Office of Research. Available at https://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf; Third, A. 2016. Researching the Benefits and Opportunities for Children Online. London: Global Kids Online. Available at http://globalkidsonline.net/tools/guides/opportunities/; 20. Livingstone, S. & Third, A. 2017. 'Children and young people's rights in the digital age: An emerging agenda' in S. Livingstone & A. Third (eds.) New Media and Society [Special Issue: Children's Rights in the Digital Age].

124 ITU (International Telecommunication Union). 2014. Measuring the Information Society Report, 2014. Geneva: ITU

125 Third, A. 2016. Researching the Benefits and Opportunities for Children Online. London: Global Kids Online. Available at http://globalkidsonline.net/tools/guides/opportunities/

126 Livingstone, S., Byrne, J., & Bulger, M. 2015. Researching children's rights globally in the digital age: Report of a seminar held on 12-14 February 2015 London School of Economics and Political Science. Available at www.lse.ac.uk/media@lse/research/Research-Projects/Researching-Childrens-Rights/pdf/Researching-childrens-rights-globally-in-the-digital-age-260515-withphotos.pdf

127 Third, A. 2016. Researching the Benefits and Opportunities for Children Online. London: Global Kids Online. Available at http://globalkidsonline.net/tools/guides/opportunities/

128 See for example Livingstone, S. & Third, A. 2017. 'Children and young people's rights in the digital age: An emerging agenda' in S. Livingstone & A. Third (eds.) New Media and Society [Special Issue: Children's Rights in the Digital Age].

129 Swist, T., Collin, P., McCormack, J. & Third, A. 2015. Social media and the wellbeing of children and young people: A literature review. Commissioner for Children and Young People, Western Australia. Available at http://www.uws.edu.au/data/assets/pdffile/0019/930502/Socialmediaandchildrenandyoungpeople.pdf; Collin, P., Rahilly, K., Richardson, I. & Third, A. 2011. The benefits of social networking services. Melbourne: Young and Well Cooperative Research Centre. Available at http://www.uws.edu.au/data/assets/pdffile/0003/476337/The-Benefits-of-Social-Networking-Services.pdf

130 Swist, T., Collin, P., McCormack, J. & Third, A. 2015. Social media and the wellbeing of children and young people: A literature review. Commissioner for Children and Young People, Western Australia. Available at http://www.uws.edu.au/data/assets/pdffile/0019/930502/Socialmediaandchildrenandyoungpeople.pdf

131 Livingstone, S. & Bulger, M. 2013. A global agenda for children's rights in the digital age. Florence: UNICEF Office of Research. Available at https://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf
Alongside generating research on the benefits and opportunities for children online, Livingstone and Bulger also identify the following priorities for global, research, policy and practice: 1) Identifying the conditions that render particular children vulnerable to risk of harm online; 2) Generating an evidence base about children's digital practice and its relationship to their rights in the global South; and 3) Evaluating existing policies and programs, and generating comparable baseline data (2013: 4).

132 Bartholet, E. 2011. Ratification by the United States of the Convention on the Rights of the Child: Pros and Cons from a Child's Rights Perspective. The ANNALS of American Academy of Political and Social Science, 633(1), 80-101. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1833621

133 Gasser, U. & Cortesi, S. 2016. 'Children's rights and digital technologies: Introduction to the discourse and some meta-observations'. Berkman Center for Internet & Society, Harvard University, Research Publication No. 2016-7. Available at http://ssrn.com/abstract=2768168

134 A Geneva Declaration of the Rights of the Child was adopted by the League of Nations in 1924 and later reviewed (1948) and adopted (1959) by the United Nations.

135 Livingstone, S. & Third, A. 2017. 'Children and young people's rights in the digital age: An emerging agenda' in S. Livingstone & A. Third (eds.) New Media and Society [Special Issue: Children's Rights in the Digital Age].

136 The Office of the eSafety Commissioner https://www.esafety.gov.au/about-the-office/role-of-the-office

137 The Office of the eSafety Commissioner https://www.esafety.gov.au/about-the-office/role-of-the-office

138 Young and Well Cooperative Research Centre https://www.westernsydney.edu.au/ics/research/projects/yawcrc

139 AU Kids Online dataset, Edith Cowan University https://researchdata.ands.org.au/au-kids-online-dataset/653422

140 Raising Children - the Australian parenting website, http://raisingchildren.net.au

141 Cyberbullying and the Bystander project ,Telethon Kids Institute, https://www.telethonkids.org.au/our-research/brain-and-behaviour/development-and-education/health-promotion-and-education/completed-research/cyberbullying-and-the-bystander-project/

142 Third, A. et al. 2014. Children's rights in the digital age: A download from children around the world. Young and Well CRC/UNICEF. https://www.unicef.org/publications/files/Childrens_Rights_in_the_Digital_Age_A_Download_from_Children_Around_the_World_FINAL.pdf
As part of the Young and Well CRC's work, a team based at Western Sydney University worked with 148 children in 16 countries to generate and analyse their insights about their rights in the digital age. The resulting report and short film were launched globally via UNICEF's channels and presented in the opening plenary of the 2014 DGD in Geneva. They have been used to advocate internationally for children's participation in the decision-making that impacts their digital practices.

143 This report featured the results of a study conducted by Western Sydney and UNICEF with children in 26 countries around the world. A separate report (Third, A. et al., 2017., Young and Online: Children's perspectives

on life in a digital world. Western Sydney University/UNICEF. https://www.unicef.org/publications/files/Young_and_Online_Children_perspectives_Dec_2017.pdf) analyses the data generated by children in depth.

144 National Children's Commissioner, 2015, Children's rights report 2015. Australian Human Rights Commission. https://www.humanrights.gov.au/sites/default/files/AHRC_ChildrensRights_Report_2015_0.pdf
Among other things, this report called on the Australian government to provide guidance to businesses about protecting children's rights in online environments.

145 Livingstone, S, Lansdown, G. & Third, A. 2017. The case for a UNCRC General Comment on Children's Rights and Digital Media: A report prepared for the Office of the Children's Commissioner of England. London, LSE Consulting. Available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Case-for-general-comment-on-digital-media.pdf

146 Digital Rights in Australia, Nov 2017, http://digitalrightsusyd.net/research/digital-rights-in-australia-report/

Acknowledgements

The State of Digital Rights Report 2018 was coordinated and produced by Digital Rights Watch, a charity organisation founded in 2016 whose mission is to ensure that Australian citizens are equipped, empowered and enabled to uphold their digital rights.

In producing this report, Digital Rights Watch worked with a number of individuals and non-profit groups. We wish to acknowledge and thank them for their hard work:

Blueprint for Free Speech
Dr Tamsin Clarke
Dr Angela Daly
Dr Suelette Dreyfus
Erin Farley
Amy Gray
Prof Gerard Goggin
Garreth Hanley
Lyndsey Jackson
Dr Monique Mann
Dr Adam Molnar
Angus Murray
Elizabeth O'Shea
Dr Kylie Pappalardo
Melanie Poole
Felicity Ruby
A/Prof Nicolas Suzor
Tim Singleton Norton
Gillian Terzis
A/Prof Amanda Third
Elise Thomas
Prof Gillian Triggs
Prof Ariadne Vromen
Dr Ian Warren

This report is also compiled from existing work in various fields of digital rights, including:

- *The Role of Encryption in Australia* - Access Now
- *Austerity is an algorithm* (Logic Magazine) - Gillian Terzis
- *Digital Rights in Australia* - Gerard Goggin, Ariadne Vromen, Kimberlee Weatherall, Fiona Martin, Adele Webb, Lucy Sunman, and Francesco Bailo - University of Sydney

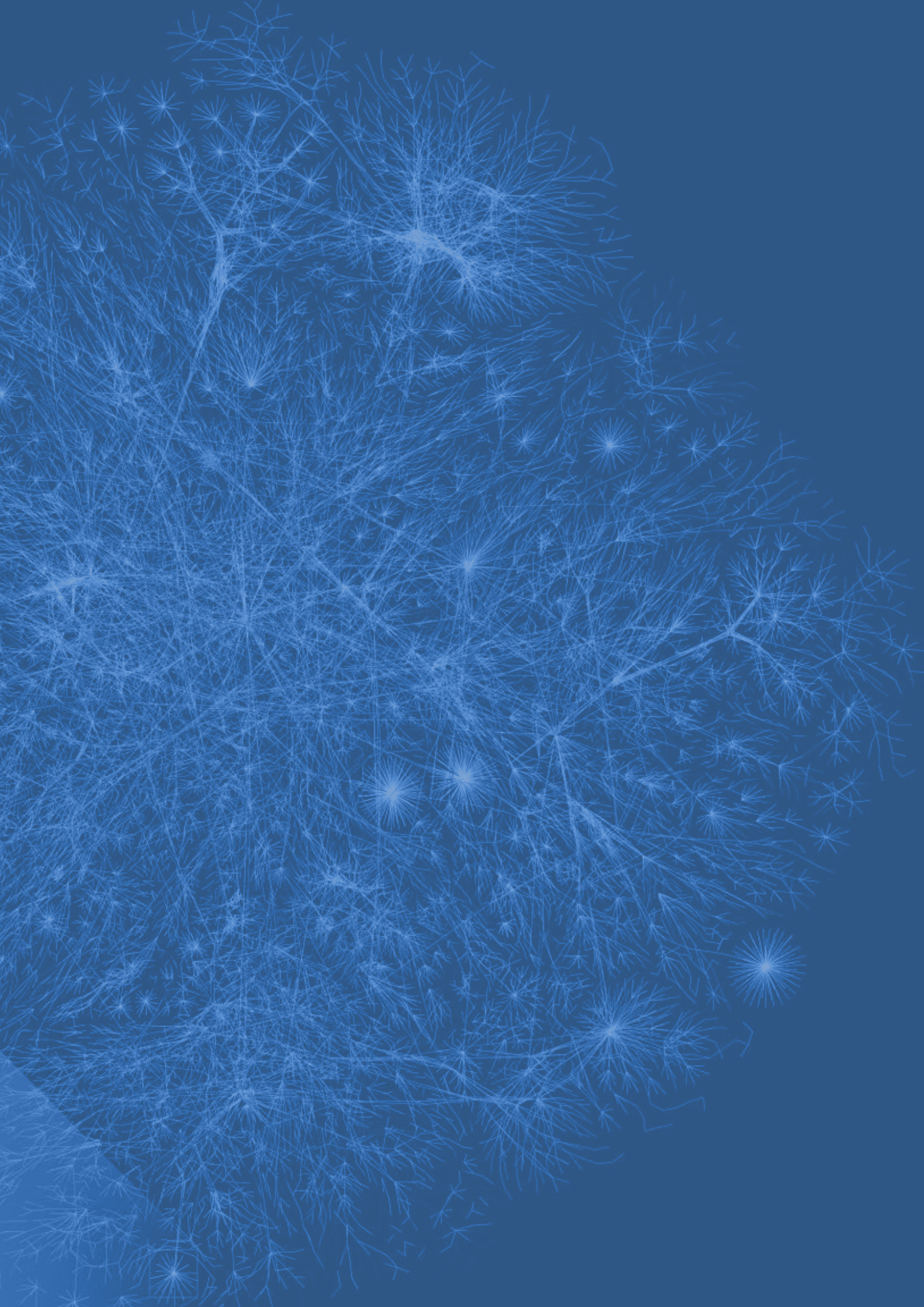
Digital Rights Watch acknowledges the traditional owners of country throughout Australia and their continuing connection to land and community. We pay our respect to them and their cultures, and to elders past and present.

Cover image: CC licensed Oliver Wunder

Endorsements

The following organisations and individuals endorse the *State of Digital Rights Report 2018*, and call upon the Australian Government to adopt the recommendations listed within:

Australian Privacy Foundation
Australian Lawyers for Human Rights
Amnesty International Australia
Blueprint for Free Speech
Castan Centre for Human Rights Law, Monash University
CryptoAUSTRALIA
Digital Rights Watch
Electronic Frontiers Australia
FutureWise
Prof Gillian Triggs
Hack for Privacy
Human Rights Law Centre
The Juice Media
Liberty Victoria
Queensland Council for Civil Liberties
Save the Children Australia
Scott Ludlam
A/Prof Tama Leaver




FIGHT
FOR YOUR
DIGITAL
RIGHTS!
netzpolitik.org