Submission to the Office of the United Nations High Commissioner for Human Rights

to the report on

‘the right to privacy in the digital age’

28 May 2021

DIGITAL RIGHTS WATCH

Overview

We welcome the opportunity to submit comments to the Office of the United Nations High Commissioner for Human Rights, addressing the right to privacy in the digital age. As an organization working on the protection of digital rights, we are increasingly concerned by the adoption of new and untested technology as human rights frameworks remain overlooked or intentionally disregarded. We view this review as incredibly timely, and we are available to the High Commissioner's office for any further inquiries pertaining to this submission.

Australia is an interesting case study for privacy in the digital age as the country continues to lack a human rights charter at the federal level. While some state governments have adopted their own, this only provides partial protection as the federal level policy remains free of those constraints. Unencumbered by human rights limitations like many other jurisdictions, the Australian government has embraced technology as the solution to a wide array of governance issues—from social welfare, to administration, and policing. Most programs come with no human rights protections or safeguards, and no avenues to address discrimination or harm.

The Australian Human Rights Commissioner has just completed his inquiry into technology and human rights, concluding there is a lack of sufficient protections for advanced facial recognition and AI systems to be used by the government.[1] Similar conversations are being had by governments around the world, where a rush to adopt technological solutions is only sometimes slowed thanks to the efforts of civil society and the human rights community.

For reference we would also like to share our submission to Australia's last UPR cycle, as well as our submissions to local reviews of the role of privacy in the digital age:

- Digital Rights Watch and Access Now joint submission to the UN Human Rights Council's Australia Universal Periodic Review (August 2020)
- Submission to Privacy Act Review Issues Paper (November 2020)
- Submission to the Data Availability and Transparency Bill (Nov 2020, Jan 2021)

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, and advocate for a digital environment where individuals have the power to maintain their human rights.[2]

[1] More in the Human Rights and Technology Final Report | Australian Human Rights Commission
[2] Learn more about our work on our website: https://digitalrightswatch.org.au/

General remarks

As the digital ecosystem grows all around us, consuming cities, workplaces, and our places of leisure and even governance, the protection of privacy has been an active frontier between human rights advocates and the reckless adoption of systems and technologies. Our right to privacy, and the ways in which we continue to interpret and demand it at the local and global level, will shape our future. And moreover, the extent of our privacy will shape our ability to pursue self-determination in an age where everything is optimised and specifically tailored to every individual; we need privacy protections to ensure that our future selves will have a right to choose and make decisions instead of being the subjects of systems and complex algorithms.

Our right to privacy is also increasingly important as governments ramp up efforts to surveil and police populations across the globe. Globalisation has brought with it an ongoing scope creep for intelligence agencies and law enforcement bodies, and national security frameworks are often altogether exempt from upholding an individual's right to privacy. While courts across Europe are adjudicating cases on data retention and mass surveillance, the rest of the world lags behind in protections for the right to privacy and any redress and justice that should accompany it.

Algorithms and optimised automated systems (and increasingly AI) are creeping into private and public services at an alarming rate. Many regulators struggle to keep pace with the language and technical dimension of the systems they are tasked with regulating. The right to privacy remains one of the most critical parts of the international human rights framework in the digital age.

Australian lack of a rights-based framework

As a part of reviewing the privacy ecosystem in Australia, we have urged the government to enshrine in law a federal level right to privacy in line with Article 12 of the United Nations (UN) Universal Declaration of Human Rights to which the Australian government is a signatory.[3] Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[4]

We believe that recognising the right to privacy at the federal level in Australia is critical. This step would create a rights-based framework with respect to the treatment of Australians' data and privacy online, as opposed to an economic or value-driven model which has been the case so far.[5] While a statutory tort for invasions of privacy has also been

[3] Australia's value-based relationship with privacy | Digital Rights Watch
[4] Universal Declaration of Human Rights | United Nations
[5] The emphasis on Consumer Data Rights (CDR) is evidence of this, as is the consideration by the Australian Bureau of Statistics to merge privately held datasets into the public census data to improve

considered as a part of multiple privacy review processes, it is yet to be implemented. Critically, it would be only a partial substitute for implementing the right to privacy outright.[6]

A rights-based approach to privacy and data protection is ensured in key jurisdictions, such as the United States, United Kingdom, and across the European Union's (EU) 27 member states, as well as signatories to the Council of Europe's Convention 108+. Matching these standards will prove increasingly critical for the Australian economy if we seek to continue cooperation and e-commerce with these jurisdictions. While we recognise that a copy and paste of the EU's General Data Protection Regulation (GDPR) may not be the appropriate solution, we would encourage the consideration of the rights guaranteed to individuals under the GDPR, many of which should form a fundamental part of a truly modernised Privacy Act. Chapter 3 of the GDPR entitled "rights of the data subject" ensures that there are clear and actionable rights for individuals.[7] The review of the Privacy Act should seek to provide the same, or similar.

The other critical weakness in Australian privacy law is that it affords most businesses and government agencies the capacity to share de-identified data without consent. The law provides no guidance on what constitutes the appropriate standards for de-identification, meaning that businesses routinely exploit this loophole to engage in data mining, and governments have released datasets of sensitive personal information from which individuals can be re-identified. The right to privacy is not inconsistent with legal regimes that permit the sharing of de-identified data, but there must be a social licence for these systems and they must be robust.

AI impact on human rights and the right to privacy[8]

Australia has had a unique experience with automated decision making through an automated debt recovery scheme the government introduced in 2016, now known infamously as 'robodebt'.[9] This automated system was originally introduced in an attempt to ensure recipients of Australian social welfare payments (called Centrelink) were not under-reporting their income and, as a result, over-receiving welfare payments. The system was designed to cross-check individuals' reported earnings with the amounts reported by a recipient's employer. The system replaced a manual human review of these data points; before the system began in 2016, there was an average of 20,000 interventions per year (or

---

results and the "economic contribution" of the census. This value-driven calculation of privacy infringement vs economic benefit fundamentally shifts when we consider a rights-based system.

[6] The Office of the Australian Information Commissioner (OAIC) has argued that even the current consideration of a statutory tort would not resolve the lack of privacy protections. More in their submission to the Privacy Act Review.

[7] More at: Chapter 3 (Art. 12-23) Archives - GDPR.eu and a user's guide by Access Now at Know your rights: How to protect your data with the GDPR - Access Now.

[8] The call for input asked for specific impacts on the enjoyment of the right to privacy caused by the use of artificial intelligence, including profiling, automated decision-making and machine-learning technologies (hereinafter referred to in short as "AI").

[9] Many articles are available online covering the lifespan of the automated debt recovery scheme. Robodebt was a fiasco with a cost yet to be fully appreciated | The Conversation

debt notices issued to welfare recipients), but with the introduction of the automated system, this number increased to 20,000 interventions per week.[10]

The system was dubbed robodebt once it became clear that the automated assessment achieved efficiency at the cost of accuracy. It resulted in assigning individuals with huge debts, often wrongly, supposedly accrued across decades, which they were unable to repay. For some it reflected acynical assessment of society's love for technology, but for many it has had long lasting mental health impacts and the scheme has been seen as linked to suicides.[11] In 2020, a class action lawsuit led to a government payout of $720 million and many critics do not view that as a sufficient amount.[12]

This dysfunctional automated scheme was only possible because of the flimsy privacy protections in place for data shared with the government. Data shared for one purpose (to submit a tax return) was repurposed to assess eligibility for welfare services. When fed into an automated process, the robodebt system produced poor decisions with little recourse for the individual in question. The upshot is that under current laws, every engagement with the state, regardless of the context, makes the citizen more visible to state authorities but not the reverse. Even though preserving an individual's privacy was not the selling point of this automated scheme, it is often the case for similar government efforts. Using a simple automated system to read paper forms and make determinations, instead of human's conducting the same task, is often portrayed as more privacy friendly as well as efficient, but robodebt proves just how wrong such assumptions are in practice. The system failed to carry out a simple function correctly, and without a manual review issued thousands of faulty debts—debts for which there were no appropriate mechanisms for feedback or appeal.

In 2019, the United Nations Special Rapporteur on Extreme Poverty, Philip Alston, published a report on digitisation where he warned precisely of the narrative of prosperity and efficiency threatening to override human rights protections. In the press release he states that, "[d]igital welfare states thereby risk becoming Trojan Horses for neoliberal hostility towards social protection and regulation.... Moreover, empowering governments in countries with significant rule of law deficits by endowing them with the level of control and the potential for abuse provided by these biometric ID systems should send shudders down the spine of anyone even vaguely concerned to ensure that the digital age will be a human rights friendly one."[13] Since Australia lacks a federally implemented charter of human rights, it is at a particular risk of these technologies as arguments by human rights activists, privacy or otherwise, often fall on deaf ears and lack the support of a judicial process that is available in other jurisdictions.

---

[10] What happens if you are overpaid by Centrelink | Crikey News
[11] Robodebt-related Trauma | The Guardian
[12] Robodebt Class Action | 7News
[13] World stumbling zombie-like into a digital welfare dystopia, warns UN human rights expert | OHCHR

Surveillance and privacy in the workplace

The right to privacy debates and policy interventions typically respond to consumer issues and the use of public space. By contrast, the workplace remains an under-analysed and complex site for regulating surveillance and ensuring workers retain a reasonable expectation of privacy. Workplace surveillance and issues of privacy are broad-ranging, and can include: disproportionate and invasive CCTV surveillance; facial-recognition; biometric data collection such as Covid-19 temperature tests, fingerprinting and voice capture; working from home monitoring tools; and medical surveillance. Increasingly this will include AI technologies as workplaces take advantage of all available modern solutions.

The workplace presents several challenges to consumer-based and individualistic language of privacy rights. This is primarily because the workplace itself is an instrument of surveillance, as it is designed to allow for oversight or supervision over the working day. This is not necessarily a problem, although there are certainly instances where managerial oversight is needlessly heavy-handed. Rather, the very nature of the workplace highlights that some degree of surveillance is inevitable or required by government regulations. As such, the task at hand is not a total ban on surveillance, but rather to determine which uses of surveillance are appropriate to the requirements of the workplace or industry, and which uses of surveillance violate a worker's right to privacy.

The distinction between appropriate and inappropriate uses of surveillance in the workplace is difficult to pinpoint for reasons of transparency and function creep. That is, employers may implement surveillance for valid reasons (such as food safety regulations) but use the surveillance footage for punitive or disciplinary purposes. The lines around what is a reasonable expectation of privacy in those instances have not been clearly drawn and are likely to lead to increased scope creep as workplaces continue in the current unregulated environment.

Government initiatives on workplace surveillance

In Australia, issues of workplace privacy and surveillance have gained considerable media and public attention following COVID-19 lockdowns and working from home arrangements in 2020. This has opened up broader conversations for local governments and unions about technology and the future of work.

On 24 March 2020 the New South Wales shadow Labor Government established the *Select Committee on the impact of technological and other change on the future of work and workers in New South Wales.*[14] The Select Committee has a focus on policy, and has held hearings with a range of stakeholders including employers, policy-makers, and unions. At

[14] More information on the Select Committee | NSW Parliament

this stage, a preliminary discussion paper of findings has been tabled.[15] Government responses to the submissions and hearings are to be determined.

Solutions and Union Initiatives

In Australia, Unions have been at the forefront of thinking through the issue of workplace surveillance but it remains a global issue. Some of the solutions that have been considered here is the adoption of:

- Clear policies regulating the scope and use of surveillance technologies in the workplace,
- Participative industrial relations system that is fit for purpose in the modern workplace,
- Privacy and technology protections in the National Employment Standards,
- Genuine worker alternatives, ability to opt-out,
- Policies to ensure new workplace technologies are co-determined with workers and unions.[16]

Conclusion

The Australian government has demonstrated a clear preference for an economic value-based calculation whenever privacy is concerned. The original authors of the Australian Privacy Act made that calculation back in the day—they asked what the economic burden of taking privacy into consideration should be. This resulted in the Privacy Act not applying to entities with an annual turnover of less than $3 million dollars, to limit the costs of privacy protections for industry. It's the same reason that the Australian Bureau of Statistics went into a lengthy consultation process in 2020 to see if they could use privately held datasets (such as electricity household usage) to supplement census data because "it creates direct value for the economy." It reflects an approach to privacy that sees it not as a right held by people, but as a potential barrier to economic growth that should be limited and contained.

This approach and calculation needs to change. Governments (and government bodies) should not be permitted to barter people's personal information away on their behalf in the name of economic pursuits. Yet this is the overarching narrative for many companies and corporations, it echoes across the halls of the World Economic Forum, and governments too easily surrender to the rhetoric that privacy is less important than implementing automated systems will make their work easier and faster—even if we have seen the contrary to be true in an extensive number of examples.

Updating the Privacy Act can give Australians the ability to control how their information is used and shared, and empower them to take action when their privacy or personal

[15] Impact of Technological Change on the Future of Work | NSW Legislative Council
[16] Technology and Power: Understanding technological change in Australian workplaces | United Workers Union

information is violated. At the moment, internationally, we are falling behind in addressing the privacy (but also broader societal and economic) harms caused by the business models of digital platforms and services, public and private alike. We have recommended the Australian federal government:

- Redefine the scope and reach of the Privacy Act.
- Update the definition of personal information.
- Adopt a rights-based approach.
- Introduce a statutory tort for invasions of privacy.
- Don't use consent as a scape-goat to weak protections of personal information.
- Abolish exemptions, namely the exemption for political messaging.
- Introduce a stronger definition of 'de-identified' data.

The time has come for Australia and other jurisdictions to recognise that privacy is a human right and not treat personal information as a bartering chip in the economy. Given the ubiquity of digital services in our lives and the amount of data collection it all entails, we must be equipped with meaningful protections and actionable human rights going forward.

Contact

Lucie Krahulcova | Executive Director | Digital Rights Watch | lucie@digitalrightswatch.org.au