CONTRIBUTION OF INPUTS TO THE
2022 REPORT ON "THE RIGHT TO PRIVACY IN THE DIGITAL AGE"

4 JUNE 2022

Contribution from:
José-Miguel Bello y Villarino
Prof Kimberlee Weatherall

To: Office of the High Commissioner for Human Rights
Via email: ohchr-privacyreport@un.org

About us
Thank you for the opportunity to inform the work of the Office of the High Commissioner on the right to privacy in the digital age. We are researchers at the University of Sydney Law School, affiliated with the Australian Research Council Centre of Excellence for Automated Decision-making and Society (ADM+S), researching questions relating to the collection and use of data, data-driven decision-making and artificial intelligence.

In this contribution we do not intend to represent the views of the organisations with which we are affiliated. We provide the following inputs in our personal capacities and based on our expertise, with the hope that they offer some insights for the report about the regulation of privacy (mainly from the Australian perspective) and the complex trade-offs for human rights that the regulation of data could involve. We would be delighted to further contribute to the work of the Office of the High Commissioner in this report or any other future work on this area.

The orientation of and basis for this submission
These comments are based on our observations of the recent Australian experience, where there has been a wide range of legislative attempts and law reform discussions aimed at adapting the existing legislation to current technological advances: especially legislation related to data about people, its collection, use, and sharing/disclosure. Specific legislation is critical in Australia, which lacks both general constitutional or legislative protection for human rights, and a common law/general law right to privacy.

We particularly look at this issue as part of the obligation of States not only refrain from violating the rights recognized in the Covenant, but, even more importantly in this context, to take positive steps to protect the enjoyment of the human rights, including privacy (A/HCR/48/31 para.10). As this High Office has previously noted, the obligation to protect "implies a duty to adopt adequate legislative and other measures to safeguard individuals against interference in their privacy, whether it emanates from State authorities or from natural or legal persons." A/HRC/39/29, para. 23).

It is obvious that the absence of relevant legislation designed to protect the right to privacy can be a violation of the Article 12 of the Universal Declaration of Human Rights and article 17 of the International Covenant on Civil and Political Rights. But the existence of laws that are **insufficient** to guarantee the relevant standards of protection can also be a violation of the international human rights commitments of States (Bello y Villarino and Vijeyarasa, 2022). It is a matter of balance and proportion: inappropriate regulation that excessively prioritises privacy protection above everything else can also deprive States of the capacity to better ensure the enjoyment of human rights.

Two themes

We wish to raise two key points, or themes, for consideration by the Office of the High Commissioner for Human Rights:

1. **Intensifying datafication** argues for more attention to aspects of data privacy that have attracted less attention in the past, especially in countries, like Australia, that have historically emphasised the role of individual consent and choice in relation to data collection and use. In particular, we would argue that more attention needs to be paid to **the right to anonymity.** Beyond data privacy, attention should be paid to aspects of the right to privacy that are not about data control as such, but **autonomy, and protection from intrusion on seclusion and on the private sphere.** These aspects of the right to privacy could justify, for example, limits on individual/micro-targeting.

2. We would urge the Office to engage seriously with **government data collection, linking, use and sharing.** Governments' increasing ability and desire to link data from different sources warrants heightened attention to governance and accountability, in order to take advantage of the potential **benefits** of such linking (including to promote other human rights) while protecting and promoting privacy. We would also urge the Office to consider the implications of government sharing/exchanging data with private entities.

Theme 1: Intensifying datafication and the importance of data minimisation and anonymity

In recent years there has been a growing realisation that ever-intensifying datafication (turning everything into data) is seriously interfering with people's, and society's, well-being. As noted in a submission to the 2021 Privacy Bill to reform the Australian regime (Goldenfein, Weatherall and Parker, 2021), strong economic incentives drive businesses to turn everything about people into data – personal information, but also activities, movements, behaviour, and even (real or inferred) emotional states. Behavioural targeting aims to make messages, goods, services, opportunities and advertising presented to people online as relevant as possible to those people, and uses ever-more fine grained information to do so. Behavioural advertising, for example, relies on data about people to price the consumer attention sold to advertisers. More, and higher quality, data about an audience increases the value of ad inventory. Publishers, advertisers, platforms and data brokers are thus incentivised to constantly procure,

acquire, and control additional data streams about individuals, and to transform as much of human life as possible into data streams that can be monetised. No one actor can eschew data collection without incurring economic disadvantage and giving the advantage to competitors. Studies show that Google has tracking technologies embedded in as much of 86% of webpages (Cyphers, 2020) and as much as 94% of Apps available in the Play Store (Statistica, 2021).

These tendencies do not only play out in well-known areas like advertising and targeting commercial products and services. Similar trends towards 'better targeting', or 'more personalised services' are playing out in a range of areas, including in high stakes contexts such as in employment and hiring services (profiling prospective employees for 'best fit'). A recent study highlighted the proliferation of data collection and profiling in education technology (edtech), and with developers building mechanisms for monitoring student attention, progress, or well-being (Human Rights Watch, 2022). This increases risks in relation to the protection of other rights, including rights against discrimination.

Individual rights to 'control' how data is used are heavily relied on in legal frameworks in Australia, and other countries, as a mechanism to protect information privacy. However, the solution to protect information privacy cannot be purely based on individual rights over their personal data and individual control over the flows of these data. Individual control may not be an effective way to promote or exercise rights to privacy, for two reasons. First, because, as is widely recognised, consent is a poor mechanism for ensuring that any use of data is voluntary on the part of individuals. Consent is frequently not genuine when presented in the form of an online tick box system that stands in the way of the consumer achieving some other goal (such as, say, booking tickets to an event); or when obtained online as a result of people agreeing to an extended written privacy policy which is unlikely to be read or understood; or where a person is not offered a reasonable alternative.

Second, obligations to provide notice of data use and obtain consent, even if strengthened, will not prevent individuals from being profiled, and will have limited impact on their information experience, or the ways in which a platform ecosystem manages their consumer behaviour. **Data is deeply relational** (Hildebrandt, 2008; Viljoen, 2021). Profiling and behavioural targeting involve the processing of data about people to identify population segments. Data used to generate inferences and profiles describe the likely consumer behaviour of an aggregate population segment, not any specific individual. Consumers who choose not to allow behavioural data collection can and will still be classified, and predictions made about them, based on aggregated data about *other* people, triggered by individual information they provide in the course of a transaction/web visit etc.

These features of the developing technological environment suggest a need to move beyond an emphasis on control and consent models for data privacy rights, and place more focus, both on *other* human rights that are impacted by new technologies (the right to freedom of association, the right to freedom from discrimination, and socio-economic

rights), but also on **other aspects of privacy rights** to which some jurisdictions like Australia have paid less attention in the past, in particular:

- **Anonymity**: the idea that individuals must have the option of not identifying themselves, or of using a pseudonym, unless it is impracticable for a data collector/controller to deal with individuals who have not identified themselves or who have used a pseudonym;
- **Decisional autonomy;** and
- Privacy as a right to protection of **seclusion from intrusion**

Anonymity is important for privacy and to protect the autonomy of individuals. For many individuals the exercise of certain perfectly legal activities or freedoms can only be confidently conducted if some degree of anonymity is present: think, for example, coordination for strikes, or protests; investigative journalism; or searching for treatments for certain diseases, among many others. Privacy is therefore equated here with the lack of capacity of one entity to identify an individual. Anonymity and the right to interact anonymously is threatened by moves to expand the verification of identity in online contexts. Australia, for example, is developing a 'Trusted Digital Identity Framework' that is explicitly aimed at being a tool for both government and business to verify the identity of people with whom they are dealing online. More widespread use of such tools, including where identity verification is not strictly necessary, threatens people's ability to make inquiries, seek information and explore opportunities anonymously.

An obligation on public and private sector entities to offer reasonable and convenient alternative ways of obtaining goods, services, benefits or information that do not require identification could protect anonymity, and also help to ensure that consent to data collection, where provided, is voluntary (if people can obtain goods or services without identifying themselves, then their decision to identify themselves can be more readily characterised as voluntary).

Decisional autonomy is attracting growing attention across a range of contexts, with some jurisdictions proposing to strengthen legal protections against attempts to manipulate people's behaviour or decision-making through the personalisation or targeting of information, communications or content: see, for example, art 5(1)(a) of the proposed EU AI Act (European Commission, 2021). Data-driven systems based on large-scale analysis of behavioural information and large-scale experimentation with interfaces, information and presentation (such as A/B testing, which is widespread online) have, as their goal, affecting the behaviour of people in ways that serve the ends of the data processor.

Finally, a long-recognised aspect of privacy is the idea that people should be free, where desired, to enjoy **seclusion against intrusion**. The need for a space free from the exercise of state power, monitoring, surveillance and judgment has been recognised as fundamental to human dignity and autonomy. This right is threatened by the growth of Internet of Things (IoT) devices and by forms of monitoring at the level of the household (such as might occur via other digitally connected devices such as electricity smart

meters and smart TV). Arguably it is also threatened by surveillance, and targeting, directed 24/7 at personal devices such as smart phones.

We suggest that there is an opportunity to think about how these more traditional aspects of privacy, beyond data privacy, have the potential to enrich our understanding of the implications of current technologies, government policy and business models, and justify limits on some surveillance and targeting activities. We argue that it is important to pay more attention to the important role of anonymity and seclusion from intrusion, and the conditions necessary for decisional autonomy.

Theme 2: Government data collection, linking, use and sharing and the need to focus on governance and accountability

Dataism is a double-edge sword to human rights: From a human rights perspective, *dataism,* the belief that every aspect of what is important about people's lives *can* be turned into data and used for prediction and control (Van Dijck, 2014), is extremely dangerous for the right to privacy. But the appropriate use of data can contribute to the realisation of other human rights and even privacy itself. The collection, and analysis of high quality data can help us identify disadvantage and cases where human rights are not being protected, or promoted, and assist governments and others to direct resources as needed to improve lives and the enjoyment of rights. Sometimes too significant benefits can be achieved by providing access to the research sector to government-held data to develop solutions to public problems. It is therefore important that an excessive focus on privacy does not prevent us from developing systems that can improve the enjoyment of the right to health, education or access to justice.

Public value of data held by public actors: Governments have become increasingly interested in making more use of the information about people and their behaviour and activities that they can access. Sometimes the value resides in data already held by public authorities for public use. At other times relevant data is held by private sector actors and sought by government: usually in aggregated form but aggregated data, as should be clear from the discussion above, can be analysed to draw conclusions about individuals.

In Australia, we have seen in recent times very significant efforts by governments to set the frameworks for, and engage in, data linkage and sharing across and between governments. There are potential benefits of these activities: as set out in a discussion paper on data-sharing (Commonwealth government, 2019): better linking, sharing, and use of data can reduce the administrative burden on citizens and residents when accessing important public services (less time spent filling out forms, repeating information to government services) and enable better informed and better targeted public policy, including where resources or interventions are required. The ability to 'drill down' into data by government can encourage more targeted interventions - not targeted at identified individuals, but at smaller subgroups in society with particular features. Past analysis, for example, of detailed, linked information about children in out of home care across a range of areas (health, education, justice etc) has made it possible to identify subgroups of children or families most at risk, or in need of the most government support.

This necessarily encourages the development of policy interventions more directly targeted at those most at risk.

The importance of safeguards and governance: That same ability to link together data held across different parts of government, and target interventions at particular groups, *is* an invasion of privacy, and confers significant power on government to affect the lives of subgroups within society. For this to conform with international human rights norms, these kind of restrictions of the right to privacy must be provided for by law, be necessary to achieve a legitimate goal, and be proportionate to that goal. As noted by that Office (A/HCR/48/31 para. 39) this means in practice that "States are required to carefully determine if a measure is able to achieve a set objective, how important that objective is [,] what the impacts of the measure will be [and] if less invasive approaches could achieve the same results with the same effectiveness; if so, those measures need to be taken". The *safeguards and governance mechanisms,* then, are critical.

Significant development of governance and accountability mechanisms for government data linking and sharing is needed: Traditional methods for holding governments and decision-makers accountable for their actions do not necessarily work with policies that are made possible by sophisticated uses of data. We know that individual privacy should be protected, but that data that could potentially involve interferences into the right to privacy could be extremely valuable for public authorities to facilitate the enjoyment of other human rights. This trade-off needs to be **continuously considered** in data-driven systems. Government organs or democratically elected institutions can exercise oversight only at the highest level, through broad principles and direct oversight is likely to occur at extended intervals. Individuals can contest the application of *individual* decisions that apply to them, but not the formulation of policy: even narrowly targeted policies or interventions with direct impacts on their lives and rights. Impacts experienced collectively require different mechanisms for governance, and accountability. The likely ineffectiveness of our usual governance and accountability mechanisms makes **the involvement of affected communities in ongoing monitoring and oversight** - **and in operations of the system -** even more important than it would otherwise be. This is especially important where data-sharing and use could impact groups or communities who are not historically represented within government or the public sector. For example, as Australia moves forward to develop the National Disability Data Asset – a cross-jurisdictional linked dataset of information about people with disability, their access to services and programs – continued involvement of people with disability in decision-making about that asset is important, to ensure their perspectives and experiences inform interpretation and decisions. In other words, ensuring ongoing respect for human rights, proportionality, legitimacy and necessity, means building mechanisms for ongoing governance of data, its use and interpretation, and involvement of affected communities in that governance and interpretation.

References

Bello y Villarino, José-Miguel & Vijeyarasa, Ramona (2022) 'International Human Rights, Artificial Intelligence, and the Challenge for the Pondering State: Time to Regulate?', *Nordic Journal of Human Rights*, DOI: 10.1080/18918131.2022.2069919

Commonwealth Government of Australia - Data Commissioner (2019), 'Data Sharing and Release Legislative Reforms Discussion Paper' <https://datacommissioner.gov.au/resources/discussion-paper>

Cyphers, Bennett, 'Google Says It Doesn't "Sell" Your Data. Here's How the Company Shares, Monetizes, and Exploits It' (2020) 10 *Electronic Frontier Foundation*

Dijck, Jose van, (2014) 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology'. 12(2) *Surveillance & Society* 197

European Commission (2021), *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) COM/2021/206 Final 2021*

Goldenfein, Jake and Weatherall, Kimberlee and Parker, Christine, Online Privacy Bill Consultation Submission (December 6, 2021). Available at SSRN:<http://dx.doi.org/10.2139/ssrn.4015915>

Hildebrandt, Mireille, 'Defining Profiling: A New Type of Knowledge?' in Mireille Hildebrandt and Serge Gutwirth (eds), *Profiling the European Citizen: Cross-Disciplinary Perspectives* (Springer Netherlands, 2008) 17 <https://doi.org/10.1007/978-1-4020-6914-7_2>

Human Rights Watch (2022) *How Dare They Peep into My Private Life?": Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic* <https://www.hrw.org/report/2022/05/25/how-dare-they-peep-my-private-life/childrens-rights-violations-governments>