

**Mandate of the Special Rapporteur on the right to privacy**

Mr. Rod Sims  
Chair  
Australian Competition and Consumer Commission  
Level 20, 175 Pitt Street  
Sydney - New South Wales  
AUSTRALIA

Dear Mr Sims,

As you will recall, I have the honour of being the United Nations' inaugural Special Rapporteur on the Right to Privacy, a role to which I was appointed in 2015 and extended last year, for a second term until 2021. As Special Rapporteur (SRP), I am mandated by the Human Rights Council Resolution 28/16 to identify possible obstacles to the promotion and protection of the right to privacy, to identify, exchange and promote principles and best practices at the national, regional and international levels, amongst other activities.<sup>1</sup>

With this responsibility forefront, I write to provide feedback on the Preliminary Report into Digital Platforms issued by the Australian Competition and Consumer Commission (ACCC) in late 2018. I note this is one of the first such reports released internationally.

First, I commend the ACCC for its well-researched report and its breadth of vision which has recognised the human right to privacy as a mechanism for the ACCC to protect, strengthen and supplement the way market competition works in Australia and to improve economic efficiency while increasing the welfare of Australians.

I note the ACCC has identified "concerns with the ability and incentive of key digital platforms to favour their own business interests, through their market power and presence across multiple markets" and the "lack of transparency in digital platforms' operations" amongst other findings.<sup>2</sup> There is significant asymmetry between the respective information and bargaining powers of digital platforms and their users. A special part of my focus is upon the very significant impact this asymmetry has upon the ability of citizenry to enjoy the fundamental human right to privacy.

I welcome and support overall, the approach and directions of the preliminary report. My primary concern is that recommendations concerning privacy for the benefit of both citizens and business, need to be placed in the larger, international context within which these digital platforms operate. Chief amongst these is the understanding of privacy as a

---

<sup>1</sup> <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>

<sup>2</sup> 2018 Australian ACCC Digital Platforms Inquiry - Preliminary Report, p1.

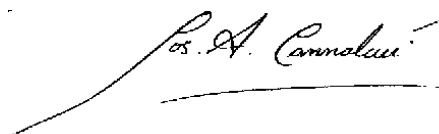
fundamental human right and the contribution of this right to democracy. The human rights framework and its enactment in privacy and data protection law enables countries to maximise the positive contributions digital platform make for individual and collective lives and to proactively address current and challenges.

In contrast to other parts of the world, Australia it seems, rarely applies this perspective to its public policy initiatives despite the enablement provided by fundamental human rights and their supporting remedial mechanisms. My concern is that the basic deficiencies in Australia's privacy framework will largely remain unaddressed despite any future adoption of the ACCC's privacy-related recommendations. The attached submission provides detail on these and other matters.

Please accept my apologies for the delay in providing this submission, I am, however, at your disposal for any consultation or information and, in addition to the UN e-mail address above, I may be contacted directly on my mobile phone +356 99 42 6133, e-mail [jcannataci@sec.research.um.edu.mt](mailto:jcannataci@sec.research.um.edu.mt). Contact can also be made with Dr Elizabeth Coombs, at [ecoom02@sec.research.um.edu.mt](mailto:ecoom02@sec.research.um.edu.mt) in relation to this submission.

I wish you every success in finalising this important Inquiry.

Yours sincerely,

A handwritten signature in black ink, reading "Joseph A. Cannataci". The signature is written in a cursive style with a long, sweeping underline.

Joseph A. Cannataci - Special Rapporteur on the right to privacy

## Preliminary Report into Digital Platforms of the Australian Competition and Consumer Commission

This submission is divided into two parts. The initial section provides background of human rights and international environment, and the second comments on recommendations. It is provided by the UN Special Rapporteur on the Right to Privacy (SRP) Professor Joseph Cannataci and the Chair, UN SRP Thematic Taskforce ‘Privacy and Personality’, Dr Elizabeth Coombs.

### Section 1: Background

1. The right to privacy is a necessary precondition for the protection of fundamental values including liberty, dignity, equality, and freedom from government intrusion, and is also an essential ingredient for democratic societies. International, regional and domestic legal frameworks for protecting the right to privacy also assist the regulation of industries with significant impact upon individuals and society. Hence, the promotion of the right to privacy is relevant to the role of digital platforms in providing news and other content and not restricted to issues of data and personal information.
2. The Universal Declaration of Human Rights calls on “every individual and every organ of society” to promote and respect human rights.<sup>3</sup> States, companies, religious bodies, civil society, professional organisations all have important roles to play. There is growing recognition that the private sector has obligations under human rights law as outlined in the UN “Protect, Respect and Remedy” Framework.<sup>4</sup>
3. Relevant to the examination of digital platforms are the experiences and views of the users of digital platforms. Research from the United States of America has found 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies.<sup>5</sup> The study concluded that privacy is not a condition of life but a commodity to purchased - presumably by those with the financial means, something which is not acceptable from a human rights perspective.
4. The everyday business practices leading to such perceptions include the difficulties of understanding companies’ privacy policies and their non-negotiability, as well as the monopoly-like nature of the social media platforms and their responses when matters of concern to users are raised.<sup>6</sup>
5. A significant matter needing consideration is the movement of major platform providers into the role of identity management via online identity authentication. Almost every website, app and service now require login details, and accepts identity

<sup>3</sup> Preamble, [https://www.ohchr.org/EN/UDHR/Documents/UDHR\\_Translations/eng.pdf](https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf)

<sup>4</sup> [https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR\\_EN.pdf](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf)

<sup>5</sup> Rainie, L. *The state of privacy in post-Snowden America*, Pew Research Centre, <http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>

<sup>6</sup> Report of the SRP Thematic Action Stream Taskforce “Gender issues arising in the digital era and their impacts on women, men and individuals of diverse sexual orientations gender identities, gender expressions and sex characteristics” – A Report of Consultation by the SRP Thematic Taskforce ‘Privacy and Personality’ in the UNSRP 2019 Annual Report to the United Nations Human Rights Council at <https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx>

credentials as authentic following logon via Facebook or Google accounts.<sup>7</sup> Facebook has 60% of this 'social log on' market and has become the de facto provider of identity validation in the non-Chinese parts of the internet.<sup>8</sup> This validation role, once the offline preserve almost exclusively of governments, has been taken up by Facebook and Google, enabling the control of access of citizens to sites and information amongst other opportunities provided by the internet. Being an identity authenticator gives digital platforms extraordinary insight into the lives of their users, and is a fundamental change in their relationship vis a vis Governments and citizens.

6. The research being undertaken by my Thematic Action Streams and by many civil society and consumer bodies confirms that the majority of customers are uncomfortable with so much of their own personal data being collected and used in ways unknown to them.<sup>9</sup> The preference for privacy and anonymity has grown as examples of data theft and the nefarious use of personal data and photographs has increased in recent years.<sup>10</sup>
7. The submissions received by the SRP Thematic Action Stream Taskforces (Big Data – Open Data; Health Data, and Privacy and Personality) confirm that the current regulatory frameworks, including privacy laws, do not effectively deter certain data practices that exploit the information asymmetries and the bargaining power imbalances that exist between digital platforms and users.
8. The Privacy and Personality Taskforce is currently examining the experiences of privacy according to gender and gender identity, and has questioned the performance of digital platforms against the obligations to protect, respect and provide remedies for the right to privacy without discrimination according to gender and gender identity.
9. The issues identified in submissions received, included:
  - i. the increased number of social media pages and groups promoting violence against women, sexism, and harmful gender stereotypes.
  - ii. the amount of community pressure it took to have these pages removed from social media platforms, although some, such as those involving children have been taken down by Facebook after official representations.<sup>11</sup>
  - iii. views of individual survivors, victims and civil society groups, Internet platforms could do more to prevent gender-based incursions into privacy regionally or globally.
  - iv. reports that the common response of private intermediaries (Facebook, Twitter, media, etc.) with respect to victims of online gender-based violence was impunity, opacity, and little proactive use of technological possibilities<sup>12</sup> such as assisting victims of abuse through apps that provide information about

<sup>7</sup> The Economist Essay, Christmas Edition, December 2018

<sup>8</sup> The Economist, Essay, Christmas Edition, December 2018.

<sup>9</sup> Pew Research Center, '7 things we've learned about computer algorithms', 13 February 2019, [http://www.pewresearch.org/fact-tank/2019/02/13/7-things-weve-learned-about-computer-algorithms/?utm\\_source=Pew+Research+Center&utm\\_campaign=ef0f933202-EMAIL\\_CAMPAIGN\\_2019\\_02\\_14\\_07\\_19&utm\\_medium=email&utm\\_term=0\\_3e953b9b70-ef0f933202-400369205](http://www.pewresearch.org/fact-tank/2019/02/13/7-things-weve-learned-about-computer-algorithms/?utm_source=Pew+Research+Center&utm_campaign=ef0f933202-EMAIL_CAMPAIGN_2019_02_14_07_19&utm_medium=email&utm_term=0_3e953b9b70-ef0f933202-400369205)

<sup>10</sup> Ritson, M., *Why you should care about the ACCC report into digital platforms*, The Australian Business Review, December 11, 2018.

<sup>11</sup> [http://www.huffingtonpost.com.au/2017/10/23/facebook-shuts-down-vile-rape-and-violence-group-linked-to-adf-troops\\_a\\_23253443/](http://www.huffingtonpost.com.au/2017/10/23/facebook-shuts-down-vile-rape-and-violence-group-linked-to-adf-troops_a_23253443/); <http://www.sbs.com.au/news/article/2017/10/24/facebook-closes-rape-meme-page-adf-troops-link> AWAV Submission, 2018; Zuckerberg, D. 2018.

<sup>12</sup> Report on the Situation in Latin America on Gender-Based Violence Exercised by Electronic Media, in de Justica, Submission, 2018.

- assistance services or using design choices, Terms of Service (ToS) and tools for reporting ToS violations and algorithmic technology.
- v. lack of transparency as to how and who inside the platforms make decisions following receipt of complaints of online violence.
  - vi. Non provision of data on the types and number of cases reported by users by country or actions taken in response. Amnesty International for example, has repeatedly called on Twitter to release “meaningful information about reports of violence and abuse against women, as well as other groups, on the platform, and how they respond to it.” Their review found that Twitter failed to adequately investigate reports of violence and abuse.<sup>13</sup>
  - vii. While the ACCC’s preliminary report largely focuses on Google and Facebook, many of the corporate behaviours described in it, particularly in relation to personal information and data generally, are characteristic of other digital/technology companies.
10. During the UN SRP consultation on the preliminary Big Data – Open Data report, suggestions were received on practical measures to help entities improve their trust relationship with users. A particular suggestion which received broad support proposed included communicating the terms of data use through standard licences akin to the six standardised Creative Commons licences. This was seen as potentially able to alleviate some of the challenges of complex privacy policies, while simplifying and standardising communication to users in different countries.<sup>14</sup> Draft licence types could be backed by more detailed ‘standard conditions’ privacy policies. It was also thought that capturing privacy risks in privacy rating labels could make privacy choices more accessible to consumers and increase the transparency and disclosure of privacy risks by data controllers.<sup>15</sup>
11. Users’ lack of awareness and understanding of the extensive information collected about them by digital platforms and the use of this data, is understandable. There is a lack of transparency in the operation of Google and Facebook’s algorithms, privacy policies are virtually incomprehensible so it is difficult for most people to make informed decisions. This opacity is common to many if not most digital offerings.
12. While this impedes potential competition between existing digital platforms and the entry of services with alternative business models as the preliminary report states, it also limits the ability of individuals, groups and communities to access and enjoy their human rights.
13. In May 2018, the European Union saw the introduction of the General Data Protection Regulation. GDPR’s influence is being exerted not just throughout Europe. Companies outside Europe, Microsoft being the most prominent example, are voluntarily adopting ‘GDPR compliance’ across their whole business operations irrespective of a legal

---

<sup>13</sup> <https://decoders.amnesty.org/projects/troll-patrol/findings>

<sup>14</sup>Submission Allens Hub for Technology, Law and Innovation, 14 August 2018.

<sup>15</sup>See Lorrie Faith Cranor, “Necessary but not Sufficient: Standardized Mechanisms for Privacy Notice and Choice”, *Journal on Telecommunications and High Technology Law* Vol 10 Issue 2, 2012, 273-308.

obligation to do so. This 'GDPR-influence' may be just as significant as legislative adoption.<sup>16</sup>

14. The increasing volume and importance of data in the digital economy means that user data increasingly impacts on competition, innovation, and consumer protection issues in Australian markets. In EU data-protection law, aspects of the GDPR provide EU consumers with new protections including greater transparency and control of data being collected about them by companies than may be provided by the EU consumer protection directives.<sup>17</sup>
15. The distinction between consumer law and data protection law is now less sharply defined<sup>18</sup> and there is advantage in strong collaboration between consumer law and privacy law. In data-driven consumer markets, the increasing use of data for developing, promoting and selling consumer products, has meant many data protection issues also become consumer issues, and vice versa.
16. The GDPR limits the use of automated decision-making in certain circumstances and requires individuals to be provided with information as to the existence of automated decision-making, the logic involved and the significance and envisaged consequences of the processing for the individual.<sup>19</sup> There is an overall prohibition (with narrow exceptions) to have decisions made by solely automated processes when such decisions have legal or other significant effects.
17. The GDPR defines profiling as the automated processing of data to analyse or to make predictions about individuals and sets an obligation to incorporate data protection by design and by default. Data Privacy Impact Assessments will be mandatory for many privacy-invasive AI and machine learning applications that fall within the scope of data protection law and have substantial anticipated risks, such as the processing of sensitive data. In the case of AI, a Data Privacy Impact Assessment could (perhaps should) enable entities to model the effects of their algorithms in much the same way climate scientists model climate change or weather patterns.<sup>20</sup>
18. The European Union Agency for Fundamental Rights has suggested one way of ensuring effective accountability could entail establishing dedicated bodies with an exclusive mandate to provide oversight of Big Data-related technologies, similar to the role of Data Protection Authorities.<sup>21</sup>

<sup>16</sup>Greenleaf, G. *Global convergence of data privacy standards and laws Speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels & New Delhi, 25 May 2018.*

<sup>17</sup>Helberger, N., Zuiderveen Borgesius, F. and Reyna, A. The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law, *Common Market Law Review*, Volume 54 (2017), Issue 5.

<sup>18</sup>Helberger, N., Zuiderveen Borgesius, F. and Reyna, A. *The Perfect Match? A Closer Look at the Relationship between EU Consumer Law and Data Protection Law*, *Common Market Law Review*, Volume 54 (2017), Issue 5.

<sup>19</sup>Articles 13, 14 and 22 of GDPR.

<sup>20</sup>The Guardian (Smith, A), *Franken-algorithms: the deadly consequences of unpredictable code* 30 August 2018, [https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger?utm\\_source=esp&utm\\_medium=Email&utm\\_campaign=Morning+briefing&utm\\_term=284469&subid=25666105&CMP=ema-2793](https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger?utm_source=esp&utm_medium=Email&utm_campaign=Morning+briefing&utm_term=284469&subid=25666105&CMP=ema-2793), quoting Johnson, N.F., Manrique, P., Zheng, M., Cao, Z., Botero, J., Huang, S., Aden, N., Song, C., Leady, J., Velasquez, N., Restrepo, E.M. *Population polarization dynamics and next-generation social media algorithms* <https://arxiv.org/pdf/1712.06009.pdf> viewed 30 August 2018.

<sup>21</sup>Fundamental Rights Agency, *#BigData: Discrimination in Data Supported Decision Making*, 2018.

19. While the ACCC's preliminary report acknowledges the impact of algorithms and AI it does not consider the contribution that may be made by provisions such as those in the GDPR. Under the GDPR, companies must identify whether any their data processing falls under Article 22 and, if so, provide individuals with information about the processing; introduce simple ways for them to request human intervention or to challenge a decision, and carry out regular checks to make sure that systems are working as intended.

## Section 2: Recommendations

The ACCC's preliminary recommendations aim to better inform consumers when dealing with digital platforms and to improve their bargaining power. The majority of preliminary recommendations are supported though there are strong concerns however, about the third-party certification proposal.

### 1. *Preliminary Recommendation 8—use and collection of personal information*

- 1.1 Support is provided for amendments to the Privacy Act to better enable consumers to make informed decisions in relation to, and have greater control over, privacy and the collection of personal information. The proposals however, do not go far enough.
  - 1.2 In the digital era the 'small business' exemption of the Australian *Privacy Act, 1988* cannot be justified. It is now possible, regardless of business size, to hold or have access to vast troves of data, the breach of which can destroy the privacy and security of countless people within Australia and elsewhere. Similarly, the exemption for employment records is inappropriate.
  - 1.3 The UN SRP consultation in Sydney in 2018 on Big Data – Open Data indicated that data protection development should, as far as possible, draw from international agreements regarded as representing 'best practice'. At present, these are the EU's GDPR and the 'Convention 108+' 2018 which originated at the Council of Europe but is open to accession globally by States which have enacted consistent principles.
  - 1.4 It is likely, in the next five to ten years, that the extraterritorial effects of GDPR with the ever-widening club of Convention 108 countries, will have a significant effect on world-wide data protection.
  - 1.5 Far greater beneficial impact upon effectively deterring certain data practices that exploit the information asymmetries and the bargaining power imbalances that exist between digital platforms and consumers, would be achieved by introducing the international standards referred to above.
2. Recommendation 8(b) *"Introduce an independent third-party certification scheme: Require certain businesses, which meet identified objective thresholds regarding the collection of Australian consumers' personal information, to undergo external audits to monitor and publicly demonstrate compliance with these privacy regulations, through the use of a privacy seal or mark. The parties carrying out such audits would first be certified by the OAIC."*
    - 2.1 This recommendation requires re-examination. It requires if retained, far greater specification as to the certification model's operations and explicitly ruling out that

certifiers' revenue streams will be dependent upon direct fee payment by those being certified. Such financial dependency would undermine the independence of certifiers, introduce perverse incentives, and invite unintended consequences.

*3 Preliminary Recommendation 9—OAIC Code of Practice for digital platforms  
A code would allow for proactive and targeted regulation of digital platforms' data collection practices under the existing provisions of the Privacy Act.*

3.1 This Code is supported to the extent that it would strengthen and refine the application of the general provisions of the Privacy Act to companies so as to secure the right to privacy and greater transparency and control over how personal information is collected, used and disclosed by digital platforms, and allow for proactive and targeted regulation of digital platforms' data collection practices under the existing provisions of the Privacy Act.

3.2 To do so, the Code of Practice requires specific obligations on how digital platforms must inform consumers and obtain consumers' informed consent, specific protections for vulnerable users, as well as appropriate consumer controls over digital platforms' data practices including the protections from differing treatment according to gender or gender identity. Broad consultation by the OAIC should occur during the process for developing this code which extends beyond that of companies and the ACCC, to the broader community.

*4 Preliminary Recommendation 10—the Government adopt the Australian Law Reform Commission's recommendation to introduce a statutory cause of action for serious invasions of privacy to increase the accountability of businesses for their data practices and give consumers greater control over their personal information.*

4.1 Recommendation supported with amendment that it is a statutory cause of action with a wider fault element for governments and corporations (encompassing intent, recklessness and negligence) and a more limited fault element for individuals (encompassing only intent and recklessness).

4.2 It is clear that within Australia, there has been considerable work done by eminent inquiry bodies at the Federal and State levels, that has seen each inquiry support the enactment of a statutory cause of action for serious invasions of privacy. These Inquiries also have included comprehensive consultation with key stakeholders. Despite these recommendations and the consultations, no Federal or State government has introduced such legislation.<sup>22</sup>

4.3 While there are a range of Australian laws that may apply to particular serious invasions of privacy, there are significant gaps in the coverage afforded to privacy protection. The lack of a cause of action specifically designed to respond to the harm arising from a serious invasion of one's privacy has resulted in awkward

---

<sup>22</sup><https://www.parliament.nsw.gov.au/lcdocs/inquiries/1877/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>



attempts to manipulate privacy claims into other actions not intended for that purpose.<sup>23</sup>

4.4 The ACCC's recommendation refers to the ALRC's 2014 report which recommended a relatively narrow in scope statutory cause of action in that it would only apply to two categories of invasion of privacy: intrusion upon seclusion; and misuse of private information. The ALRC's earlier 2008<sup>24</sup> and the NSWLRC's 2009 report supported a broad cause of action that was not limited to invasions of privacy in the nature of intrusion upon seclusion or misuse of private information. As usefully pointed out in the 2016 Inquiry undertaken by the NSW Parliamentary Committee, in its discussion of fault, it is unlikely that big data breaches would meet 'intention or recklessness' thresholds.<sup>25</sup>

## 5 *Preliminary Recommendation 11—unfair contract terms*

5.1 Support is provided for the proposal to ensure that privacy policies are not vehicles for unfair contract terms.

---

<sup>23</sup> Ibid.

<sup>24</sup> Australian Law Reform Commission, Report 175, 2008.

<sup>25</sup> <https://www.parliament.nsw.gov.au/lcdocs/inquiries/1877/Report%20no%2057%20Remedies%20for%20the%20serious%20invasion%20of%20.pdf>, particularly pts 4.33-4.36.