The Treasury
DPIConsultation@treasury.gov.au

Re: Digital Platforms Inquiry

September 12, 2019

To Whom It May Concern -

Thank you for this opportunity to provide comments to the Australian Treasury in reaction to the Australian Competition and Consumer Commission's (ACCC) report on Digital Platforms. Though our submission, we wish to emphasize the importance of human rights in the digital space and the key role that ACCC's report can have on Australian's rights going forward.

Access Now is an international non-governmental organization founded in 2009 to extend and defend the digital rights of users at risk.[1] Access Now provides policy recommendations to leaders in the public and private sectors to ensure the Internet's continued openness and the protection of fundamental rights. We engage with an action focused global community from more than 185 countries, and our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.

We are writing this in response to the Government inviting submissions on the final report of the Australian Competition and Consumer Commission's (ACCC) Digital Platforms Inquiry: "we are seeking stakeholder comments on the ACCC's findings and recommendations. In particular, we would welcome views on practical options for implementation, timing and any impediments or challenges."[2]

In our submission below, we will focus on commenting on recommendations 15, 16, 17 and 19 which focus on content monitoring and data protection/privacy given their particular relevance for the advancement of individuals' rights and our expertise on these matters.

**Recommendation 15**: Digital Platforms Code to counter disinformation

The ACCC's inquiry correctly lead them to identify the impact of disinformation on democracies and the way in which social media and advertising algorithms can be abused in the spread of illegal content. We support the proposed concept of a complaint mechanism to be enforced by an independent authority, though we would like to highlight the need to fully understand and account for threats which this mechanism could pose to freedom of expression of Australian individuals.

[1] More information can be found at: https://www.accessnow.org/
[2] In reference to: https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry

In October 2018, Access Now together with Civil Liberties Union for Europe, and European Digital Rights (EDRi) published a joint report evaluating the European Commission's online disinformation and propaganda initiatives.[3] The report encouraged good policy development based on thorough research and evidence. We advised that the European Commission or EU Member States should not propose binding policies until evidence and accurate benchmarks have been identified.

Together we warned against some of the proposed solutions by the Commission. Example of such flawed solutions are institutionalised fact-checking, relying on blind faith in Artificial intelligence and emerging technologies, creating the "EU vs. Disinformation" campaign and limiting anonymity.[4] We would advise that in its interpretation of the ACCC's recommendation, Australia steers away from similar simplified solutions as well.

As a possible way forward, our joint report advocates for three more meaningful solutions.

1. Address the business model of online manipulation through appropriate data protection, privacy and competition laws.
2. Prevent the misuse of personal data in elections.
3. Increase media information and literacy.

In May 2019, we published a discussion paper on human rights principles for content moderation at scale.[5] The paper lays out principles and recommendations for engaging in content moderation practices in a manner that is compatible with international human rights standards. It also includes an analysis of Facebook's proposed independent oversight board which was in part a reaction to the global push for content moderation after the tragic events in Christchurch earlier this year. We have been an active part in the multi-stakeholder discussion of the Call and while there is much about the approach to appreciate, we have cautioned against the adoption of ill-defined requirements on service providers as well as the need to steer from an overreliance on automated tools.[6]

**Recommendations 16 and 17**: Strengthen protection in the Privacy Act and Broader reform of Australian privacy law [7]

The ACCC's conclusions on the need for a broad reform of the Privacy Act to better serve consumers is supported by arguments made for several years by academics and interested

[3] The pdf of the full disinformation report can be viewed at: https://dq4n3btxmr8c9.cloudfront.net/files/2r7-0S/online_disinformation.pdf
[4] Full statement about the report launch can be viewed at: https://www.accessnow.org/civil-society-calls-for-evidence-based-solutions-to-disinformation/
[5] The full paper on human rights principles for content moderation at scale is accessible at: https://www.accessnow.org/free-expression-at-scale-a-human-rights-guide-to-content-moderation/
[6] Access Now breakdown of what the Call gets right and what needs improvement can be found here: https://www.accessnow.org/access-now-on-the-christchurch-call-rights-wrongs-and-whats-next/
[7] We provide comment on the two recommendations together as we believe they should be addressed and treated simultaneously to ensure successful protections for individuals' privacy.

civil society organizations.[8] The Privacy Act dates back from the pre-internet era and although the original text has been amended and updated over time, it is not fit to protect individuals offline and online. The scope of the law is limited to Australian Government agencies and private entities with an annual turnover of more than $3 million, as well as some health organisations. This means that a large number of private entities processing data do not have obligations under this law. This lack of harmonised rules has also led to the development of a patchwork of privacy protections for consumers across Australia. In addition, the law gives very little power and rights to individuals; rather it has created a set of boxes to tick for those companies which are regulated by the Act. Most notably, individuals are not empowered to challenge infringements upon their rights, nor are entities required to inform individuals or held responsible for the privacy impacts of breaches which resulted in personal data being compromised.

The recommendations put forward by the ACCC in order to strengthen the Privacy Act -- from updating definitions, to refining consent requirements and introducing redress mechanisms -- would bring Australia closer to current global best practices and would ensure that Australian entities stay in step with their international partners. Protecting privacy and personal data is not only necessary to guarantee the rights of people in Australia but a prerequisite to ensure secure flow of data which are at the center of the global digital economy.

In our 2018 submission to the ACCC's consultation on this matter, we recommended an overhaul of existing privacy rules -- both for the government sector and for industry.[9]

Last year, we published a report entitled *Creating a Data Protection Framework: A Do's and Don'ts Guide for Lawmakers* in which we elaborated on our experience with the legislative process of the EU's General Data Protection Regulation (GDPR). One of the key components is the need to create binding data protection principles in the law. We propose eight key "minimum standard" principles derived from existing international standards, in particular Council of Europe's Convention 108 and the OECD guidelines.[10] The principles are: fairness and lawfulness, purpose limitation, data minimisation, accuracy, retention limitation, individuals' rights, integrity and confidentiality and adequacy. These principles should be the basis of any data protection framework and are present in a large number of data protection laws around the world, from the EU GDPR, and most data protection laws that are in place in Latin America and Africa.

In considering the creation of a data protection and privacy framework through the reform of the Privacy Act, the government should do an audit of other existing legislation which involves processing of individuals' data and consider amendments in order to ensure that

---

[8]https://www.theaustralian.com.au/business/business-spectator/news-story/privacy-act-revisions-little-bark-no-bite/48a60ffc989d27dabfdef60ad281b368

[9] https://www.accc.gov.au/focus-areas/inquiries/digital-platforms-inquiry/submissions/submissions

[10] Organisation for Economic Cooperation and Development, September 1980. Guidelines governing the protection of privacy and transborder flows of personal data: https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/OECD_Privacy_Guidelines_1980.pdf

privacy protections are harmonised across the board. For instance, there is a current review by the Parliamentary Joint Committee on Intelligence and Security over the data retention requirements imposed on telecommunications and internet providers. In order to ensure the privacy of individuals, the data retention requirement should be reviewed in line with international standards, including the necessary and proportionate principles.[11] [12]

In our data protection report we further recommend that the following rights are made binding in any future data protection and privacy law in order to protect individual users' rights:

1. **Right to access** enables users to obtain confirmation from services and companies as to whether personal data concerning them have been collected and are being processed. If that is the case, users shall have access to the data, the purpose for the processing, by whom it was processed, and more.
2. **Right to object** enables users to say "no" to the processing of their personal information, when they have not given their consent to the processing of their data nor signed a contract. This right to object applies to automated decision-making mechanisms, including profiling, as users have the right not to be subjected to the use of these techniques.
3. **Right to erasure** allows users to request the deletion of all personal data related to them when they leave a service or application.
4. **Right to rectification** allows users to request the modification of inaccurate information about them.
5. **Right to information** ensures that users receive clear and understandable information from entities processing their personal data, whether these entities have collected this information directly or received it through third parties. All the information provided to the user shall be provided in concise, intelligible, and easily accessible form, using clear and plain language. This information shall include details about data being processed, the purpose of this processing, and the length of storage, if applicable. The entities shall provide their contact details and an email address to allow users to contact them in case there are issues.
6. **Right to explanation** empowers users to obtain information about the logic involved in any automatic personal data processing and the consequences of such processing. This right is crucial to bring accountability and transparency in the use of algorithms to make decisions that impact users' lives.
7. **Right to portability** enables users to move certain personal data they have provided from one platform to another offering similar services. To facilitate this process, interoperability between services shall be encouraged.

Rules for the transfer of data to third countries are equally necessary. Data protection frameworks are designed to ensure the free flow of data by establishing adequate mechanisms for data transfer and effective safeguards for individuals' rights. These

[11] The joint submission by Human Rights Law Center, Access Now and Digital Rights Watch filed in July 2019 can be found on the PJCIS website: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Submissions

[12] The full text of the principles is available at: https://necessaryandproportionate.org/principles

mechanisms must be put under strict and transparent oversight and include effective remedies to ensure that the rights of individuals travel with the data.

Finally, no privacy and data protection framework can be complete without a robust enforcement mechanism which includes an independent supervisory authority (data protection authority -- DPA -- or commission). Even the best data protection law in the world would be close to meaningless without an authority having the powers and resources to monitor implementation, conduct investigations, and sanction entities in case of data protection violations. Sanctions should be proportionate to the violations and can be in the form of notice to action accompanied with punitive fines.

Though there is likely to be strong pressure from industry, we would strongly caution against resorting to self-regulation and co-regulation mechanisms as an alternative to conducting a thorough reform of the Privacy Act. Despite several attempts around the globe, there are no examples of successful non-binding regimes for the protection of personal data or privacy that have been positive for individuals' rights or, indeed, business as a whole.

**Recommendation 19**: Statutory tort for serious invasions of privacy

One of the key components of a functional privacy or data protection regime is the ability for individuals' rights to be enforced and for individuals to seek remedy. Establishing a statutory tort for invasions of privacy would greatly extend individual's ability to exercise their rights and keep companies accountable. The creation of a tort for serious invasions of privacy was already recommended by the Australian Law Reform Commission in 2014, since then the need for such avenue has increased as data harvesting practices are skyrocketing in Australia.[13]

Among the most serious risks facing individuals today are the routine over-collection practices of entities and the breaches of personal data that contribute to identity theft, financial fraud, discrimination and other economic and non-economic harms. Individuals should be able to pursue a private right of action that produces meaningful penalties. Statutory damages for violations of privacy obligations should be an essential element of an effective data protection and privacy law in Australia.

As more data are being shared online and off, it is high time to develop mandatory frameworks for data protection and privacy all around the world to prevent or end these behaviours and put individuals back in control of their information. This will also enable the development of privacy-friendly innovation which is currently limited to a small number of companies that have undertaken a long-term engagement approach to protect their individuals instead of basing their business model in monetising individuals' private information.

[13] The recommendations in that report can be accessed at: https://www.alrc.gov.au/publication/serious-invasions-of-privacy-in-the-digital-era-alrc-report-123/recommendations-17/

**Conclusion**

We appreciate the opportunity to further comment on the report published by the ACCC as the government considers its next steps with regard to digital platform regulation. While there is plenty of well researched and articulated policy in the report to follow, we recommend that the best way to protect users and prevent predatory business practices is through the implementation of comprehensive data protection or privacy regulation, including a right to access, right to portability right to information, right to object, right to rectification, and a right to explanation. This comprehensive regulatory framework should also be applicable to all industries.

We remain at your disposal for any further inquiries regarding this consultation or our submission.

Thank you,

Lucie Krahulcova, Policy Analyst for Australia and Asia Pacific | lucie@accessnow.org
Estelle Massé, Senior Policy Analyst | estelle@accessnow.org