Australian Competition and Consumer Commission
platforminquiry@accc.gov.au

Re: Digital Platforms Inquiry

April 3, 2018

To Whom It May Concern -

Thank you for this opportunity to provide feedback to the Australian Competition and Consumer Commission (ACCC) regarding the Digital Platforms Inquiry. We wish to emphasize the importance of human rights in the digital space.

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.

The ACCC seeks feedback on a number of specific questions (the Terms of Reference) on the topic of "*the impact of digital search engines, social media platforms and other digital content aggregators (platform services), on the state of competition in media and advertising services markets, in particular in relation to the supply of news and journalistic content, and the implications of this for media content creators, advertisers and consumers*."[2] Specifically, our responses highlight the importance of data protection and the digital rights impact of the "over-the-top" debate as well as the impact of regulation on the human right to freedom of expression.

Social Media and Data Protection

The ACCC has asked:

> 3.4(c) What difficulties do users encounter in switching between platforms? Do digital platforms engage in behaviour that makes switching between platforms more costly or more difficult for users?

[1] accessnow.org/.

[2] https://www.accc.gov.au/system/files/DPI%20-%20Issues%20Paper%20-%20Vers%20for%20Release%20-%2025%20F.._%20%28006%29.pdf.

3.20. What terms and conditions govern consumers' use of digital platforms? How do they differ from those which apply when consumers obtain news and journalistic content from other sources?
3.21. Are consumers generally aware of these terms and conditions? Specifically, do Australian consumers understand the value of the data they provide, the extent to which platforms collect and use their personal data for commercial purposes, and how to assess the value or quality of the service they receive from the digital platforms?
3.23. If you consider the collection of data part of the effective price paid by consumers for use of the digital platforms, to what extent are consumers aware of and provide informed consent for the collection and use of their data?
3.25. How do consumers value digital platforms' access to their data? Do consumers see it as a cost or a benefit (e.g. it enables customisation of the content displayed)? How does the access to or control over user data impact the relationship between digital platforms and consumers?
3.36. Are the existing laws and regulations sufficient to address the activities of digital platforms? Is there a case for the specific regulation of digital platforms and, if so, what issues would proposed regulation seek to address?

People produce digital footprints at an alarming rate. Almost everything we do online or off can be — and often is –- tracked by digital platforms. For example, already by 2012 Facebook was collecting about 180 petabytes of data per year.[3] This growth in large scale collection, retention, transfer, and analysis of personal data places everyone's privacy at risk. The recent news about the ability of Cambridge Analytica to gain access to the Facebook data of 50 million users (and retain that data despite requests by Facebook to delete it) demonstrates some of the potential harms from business practices based on user information.[4] Cambridge Analytica is a company headquartered in the United Kingdom that has been noted for its role in interfering and manipulating elections globally.[5] The latest scandal highlights the company's intervention in United States elections, where Cambridge Analytica's activities were bolstered by targeted advertising made possible because of its access to this data.

---

[3] *Id*. For reference, one petabyte is the equivalent of 20 million 4-drawer filing cabinets filled with text.
[4] *See,* https://www.accessnow.org/its-not-a-bug-its-a-feature-how-cambridge-analytica-demonstrates-the-desperate-need-for-data-protection/ ("The story begins in 2014 when a group of social scientists led by Aleksandr Kogan created and deployed a personality test called "thisisyourdigitallife" via a Facebook app. This app allowed researchers to access personal information not only about app users but also their Facebook friends. These friends had not used the app and therefore could not have consented to the use of their data. This feature allowed Kogan and his team — along with potentially any other researcher with similar access — to harvest the information of a vast network of Facebook users. In this case, reports indicate that 50 million people could have had their data mined by Kogan (a couple hundred thousand "consenting" users and all of their contacts).").
[5] https://www.channel4.com/news/cambridge-analytica-revealed-trumps-election-consultants-filmed-saying-they-use-bribes-and-sex-workers-to-entrap-politicians-investigation.

This incident also demonstrates that digital platforms are not the only threats to people's privacy. Other consumer facing companies, third party data brokers, government agencies, and others develop comprehensive profiles at times containing information that may be sensitive, such as names, addresses, and phone numbers, as well as buying habits, personal interests, ethnic identities, political affiliations, marital status, credit card details, and numerous other data points.[6] Enough information is often collected that even anonymous information can be easily reidentified.[7]

Pursuant to international law and UN Guiding Principles on Business & Human Rights, elaborating the UN Ruggie 'Protect, Respect, Remedy' Framework ("Ruggie Principles"), all companies have the responsibility to understand the impact of their products and services on human rights, locally and globally. Companies should take measures to prevent and mitigate any adverse impacts they cause or contribute to, including through conducting human rights due diligence, consulting external stakeholders from affected communities, and developing rights-respecting policies addressing their priority human rights risks. The third pillar of the Ruggie Principles states that companies and governments should jointly provide affected persons with meaningful access to remedy for any business-related harms.[8]

Unfortunately, platforms primarily rely on terms of service to inform users, which typically consist of lengthy, abstract provisions written in heavy legal jargon. Not even the most sophisticated users today have a meaningful understanding of the content or meaning of these documents, including how their data is manipulated; how to contact platforms for appeal when their accounts are suspended or their content gets taken down; or how to prevent their data from being spread and sold across the internet.[9] Because of this, terms of service cannot provide adequate transparency or accountability for users. This scenario calls for a radical change in the way we protect personal data not only from digital platforms, but all entities.

The lack of understanding or power among internet users belies the growing capacity of those hoarding and processing their data. As Tim Berners-Lee, credited as the creator of the World Wide Web, observed, platforms like Facebook have enabled the web to be weaponized at scale, to the detriment of users' rights and the health of our democracies.[10] Data protection is

---

[6] https://newrepublic.com/article/115041/what-big-data-does-and-doesnt-know-about-me.

[7] https://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/#3d52f3e992c9. In one high profile case, reporters were able to identify several anonymous users based solely on their AOL search history, which had been publicly released. https://www.nytimes.com/2006/08/09/technology/09aol.html?pagewanted=all. Information in one user's records provided detailed information on her medical history and love life.

[8] http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

[9] *See, e.g.*, http://www.adweek.com/digital/survey-many-users-never-read-social-networking-terms-of-service-agreements/; https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print; https://arstechnica.com/tech-policy/2016/07/nobody-reads-tos-agreements-even-ones-that-demand-first-born-as-payment/.

[10] https://qz.com/1226520/tim-berners-lee-the-web-is-being-weaponized-lets-fight-for-its-future/.

vitally important for disarming that capacity and creating a better future for everyone.[11] Data will not be adequately protected absent robust, standardized, and consistently-enforced regulation.

Access Now has worked on data protection legislation across the world since 2009. Much of our data protection work has focused on the EU reform that led to the adoption of the General Data Protection Regulation (GDPR).[12] We have also tracked the progression of data protection legislation around the world, including in Tunisia, India, and Argentina, all of which are currently considering passing or updating laws.[13] Through these experiences, our organization have learned that protecting users' data and guaranteeing control over personal information requires establishing a series of binding rights. One of these rights is the right to portability, which ensures that users are able to move between platforms once interoperability is developed. In light of the GDPR, several platforms are already starting to offer this capability, greatly contributing to the rights of all users. However, it's not enough. Among other rights a data protection law must provide for include a right to access, right to information, right to object, right to rectification, and a right to explanation.[14]

Regulating Over-the-Top Services

The ACCC has asked:

> 3.34. Should digital platforms be subject to the same laws and regulations as other market participants in the media and advertising services markets (e.g. news and journalistic content creators or distributors)?

Technically, any content or services that ride on top of the network layer without the direct control or commercial distribution by network operators are Over-The-Top (OTT) services: jargon for services that run "on top" of the telecommunications networks -- the phone, cable, or satellite networks that existed before the internet. OTT services include applications like WhatsApp and Netflix, which often compete with similar services based in these traditional networks, such as SMS messages or television companies.

The internet has shown to be a force for social and political change.[15] It enables billions of people around the world to express themselves and to access information. That information

---

[11] For Access Now's Guide on the Do's and Don'ts of Data Protection Frameworks, *see* https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf.

[12] European Union, Regulation 2016/679/EU on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[13] *See*, *e.g.*, Tunisia national authority for the protection of personal data. Projet de loi relative à la protection des données personnelles (2017), *available at* http://www.inpdp.nat.tn/Projet_PDP_2017.pdf.

[14] https://www.accessnow.org/cms/assets/uploads/2018/01/Data-Protection-Guilde-for-Lawmakers-Access-Now.pdf.

[15] https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/.

includes educational resources and cultural goods. The internet can also improve our economic well being by enabling the trade of goods and services and the creation of innovative new businesses.[16] All of these activities are expressions of our digital rights.

Despite this, proposals around the world have argued that OTT services — comprising many of the internet applications and services that we all use everyday — should be regulated in a manner similar to legacy telecommunications and internet access provider services. However, initiatives to establish telecom sector-style regulation of "OTT" services are likely to have a significant, adverse impact on users' rights, including rights to free expression and access to information, and the capacity of societies to harness the internet's benefits for economic, social, and cultural development.[17]

Regulatory regimes should be fit-for-purpose. We ought not to apply telecom-style licensing regulations to internet services or mobile apps — even those offering online communication services — if they are not being launched or commercially offered as telecom services (which are precisely defined in most national telecommunications legal frameworks). This would subject them to licensing requirements or pre-government authorisations specific to the telecom or broadcast sector, and this can harm free expression and the open internet.[18]

Safeguarding the Right to Freedom of Expression

The ACCC has asked:

> 1.5. What are appropriate metrics for measuring the choice and quality of news and journalistic content?
> 3.24. Have digital platforms changed the quality or choice of media content supplied to Australian consumers? Has the use of algorithms to select content changed the diversity of news supplied to consumers?

As freedom of expression enables advocacy for a range of human rights, safeguarding freedom of expression is key to advancing other human rights. But access to information and freedom to impart information is not just socially important. It also has a significant positive economic and political impact. Protecting the right to the freedom of expression has been central to Access Now's work throughout our history.

---

[16] http://www.pewresearch.org/fact-tank/2015/03/19/key-takeaways-technology-emerging-developing-nations/.

[17] For example, placing additional restrictions on the ability for users and other actors to easily create and distribute web content will likely result in less locally relevant content on the internet, in turn impacting its overall value as well as failing to address demand related factors that would otherwise have helped increase internet uptake.

[18] https://www.accessnow.org/cms/assets/uploads/2017/08/Access_Now_OTT-position%E2%80%93paper.pdf.

Governments around the world are pushing digital platforms like Facebook, Twitter, and Google to "do more" to remove bad content and safeguard so-called "legitimate journalism." Unfortunately, the proposals to address these issues have ranged from the dreadful to the truly atrocious, typically focusing on ways to block or filter out the "bad" stuff. This has significant implications for free expression and the future of the open internet.

Internet communications tools and social media platforms have provided people with untold opportunities. Around the world, journalists, including bloggers and citizen journalists, use internet platforms to share information, connect, and organize. However, the internet does not distinguish "good" from "bad" uses of these tools or platforms. When governments see an increase in what they consider "bad" activity, officials around the world often respond by asking platforms to "voluntarily" restrict dissemination of specific content. In this way, governments coerce platforms to assume the role of police, judge, and jury of online content. They compel platforms to proactively manage content, either by advancing new legislation or by threatening to censor speech outside of the legal process. Too often, governments pressure platforms to take swift action against content outside due process mechanisms or the rule of law.[19]

At the most extreme, these government legislative proposals mandate platforms monitor, interpret, police, and (sometimes) block user content. For example, Germany recently enacted the "Enforcement on Social Networks" law, commonly known as "NetzDG." This law requires social media platforms to remove hate speech within 20 hours to seven days, depending on the difficulty of the content evaluation. If a platform fails to remove hate speech, within the established timeframe, they may be subject to a 50 million euro fine.[20] Such severe penalties tip the scales toward blocking and have a chilling effect on freedom of expression rights.

In addition to seeking to over-regulate content, many government proposals seek privatized enforcement for speech laws, delegating the role of censor to private companies without adequate judicial oversight or public accountability. And, either by pushing for direct regulation or privatised enforcement, one of the primary proposals has been to promote only "legitimate" journalism, at the expense of other sources.

"Citizen" or unprofessional media workers and entities often play critical roles in news investigations and disseminating information. This means any preference of one type of content over the other will interfere with the human rights to privacy and freedom of expression. Ever-shifting standards for removal often change without transparency. Additionally, when any type of content is disfavored, statistics show that platforms will often remove much legitimate

[19] https://www.accessnow.org/edri-access-now-withdraw-eu-commission-forum-discussions/.
[20] Lomas, Natasha. Germany's social media hate speech law is now in effect. TechCrunch, TechCrunch, Oct. 2, 2017, techcrunch.com/2017/10/02/germanys-social-media-hate-speech-law-is-now-in-effect/, (last visited Jan. 8, 2018).

content as well.[21] In either case, human rights would suffer, and the censorship is likely to have the worst impact on already marginalized populations.

Conclusion

While the current environment may seem to signal the need to limit certain types of speech and create new regulations for digital platforms, there are many ways these actions will undermine human rights and harm users. The best way to protect users and prevent predatory business practices is through the implementation of comprehensive data protection regulations, 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.

Thank you,

Naman M. Aggarwal, Asia Policy Associate | naman@accessnow.org
Estelle Massé, Senior Policy Analyst | estelle@accessnow.org
Amie Stepanovich, Global Policy Counsel | amie@accessnow.org

[21] For example, Governments intensifying the pressure on companies to deal with “extremist content” has also led to this kind of removal, such as when YouTube removed videos documenting the war in Syria.