Submission

Senate inquiry into international digital platforms operated by Big Tech companies

Mark Nottingham
Prahran, Victoria
26 February 2023

Thank you for the opportunity to make a submission.

I have been involved in the development of the Internet and the World Wide Web for over twenty years, contributing to and holding leadership roles in both the Internet Engineering Task Force (IETF)[1] and the World Wide Web Consortium (W3C).[2] A series of Silicon Valley companies have sponsored that work.

I have also recently been selected as an expert advisor to the UK Competition and Markets Authority's Digital Markets Unit,[3] and hold a Graduate Diploma of Communications Law from Melbourne Law School.[4]

Like many of my colleagues who help to develop and maintain the Internet and the Web, I am deeply concerned about their misuse — whether that be the various harms experienced by its users, or as seen in the abuses of power that 'big tech' companies sometimes evidence. The public debates about what to do about these ill effects has been mirrored in the private bodies that help to govern the Internet, where there is broadening recognition that legal regulation plays an important role.

At the same time, I am concerned about the potential for negative effects by well-intentioned regulation that does not take the Internet's architecture, history, and fragility into account. Poorly designed regulation could make global Internet fragmentation more likely; or, it might create forces that create barriers to evolution of technology — including unintentionally 'locking in' the dominance of big tech.

With that context in mind, please find my responses to selected questions below.

---

[1] See <https://www.ietf.org/about/introduction/> for more information about the IETF.

[2] See <https://www.w3.org/Consortium/> for more information about the W3C.

[3] United Kingdom Competition and Markets Authority, "Experts appointed as UK looks to level digital playing field for consumers" (Press Release, 23 February 2023) <https://www.gov.uk/government/news/experts-appointed-as-uk-looks-to-level-digital-playing-field-for-consumers>.

[4] See <https://www.mnot.net/personal/resume/> for more details of my background.

Market Concentration

Question 2: What regulatory measures could be put in place to address the adverse impact of big tech companies? What other non-regulatory interventions could governments take to reduce the market power of big tech companies?

Much has been written about taming big tech with interoperability mandates.[5] While requiring companies with undue power to 'open up' interfaces is not a panacea, it does show great promise: not only would doing so open up opportunities for competing companies, but (if correctly applied) it would allow users to manage their data directly, without a commercial intermediary.

This approach is in keeping with the architecture and historical examples of the Internet and the Web themselves. Openly specified, interoperable protocols and formats brought us these public goods and helped to assure that no single party had control over them.[6] Legal pressure to provide interoperable interfaces to specific functions identified as 'chokepoints' for power — e.g., when there is an imbalance in power due to network effects — has the potential to do the same for social networking, shopping, chat, and other proprietary functions that have been built on top of the open Internet.

However, it is necessary to recognise that writing successful interoperable specifications requires considerable expertise, and the specification process itself is a risk for abuse of power, since it can provide or withhold various capabilities that advantage or disadvantage parties. So, while big tech companies have the technical expertise to write these specifications, allowing them to do so is clearly unworkable because the outcomes will be heavily biased towards their needs, not competitors' or society's.

Instead, existing international and open Standards Development Organisations (SDOs) like the IETF and W3C are the most suitable venues for creating interoperability specifications. They have the necessary expertise, a proven track record, are transparent, and have reasonable processes for avoiding domination by any one concern. Importantly, civil society organisations, academics and governments are already represented in their work.

For example, the IETF MIMI Working Group[7] has just been created. If it successfully delivers an appropriate specification, this should address the interoperability requirements for messaging created by the European Digital Markets Act.

---

[5] See, eg, "Considerations for Mandating Open Interfaces", Internet Society (December 2020) <https://www.internetsociety.org/resources/doc/2020/white-paper-considerations-for-mandating-open-interfaces/>; Ian Brown, "Interoperability as a Tool for Competition Regulation", Open Forum Europe (November 2020) <https://openforumeurope.org/publications/ofa-research-paper-interoperability-as-a-tool-for-competition-regulation/>; "Data Portability, Interoperability and Digital Platform Competition", OECD (2021) <http://oe.cd/dpic>.

[6] See also Mark Nottingham, "Internet Consolidation: What can Standards Efforts do?" (Work-in-Progress, 17 January 2023) <https://www.ietf.org/archive/id/draft-nottingham-avoiding-internet-centralization-08.html>.

"More Instant Messaging Interoperability (mimi)" <https://datatracker.ietf.org/group/mimi/about>.

It is important to note that relying on an open technical standards development process is not a guarantee of success — SDOs only provide a global forum for discussion and consensus within well-understood rules, albeit one where the relevant technical expertise is present. And, since they produce voluntary standards, not legal mandates, care should be taken to avoid granting them undue powers (e.g., by requiring adoption of their output prematurely).

Instead, a clear but non-specific regulatory (or legislated) requirement for an interoperable interface in a targeted domain (e.g., messaging, social networking) along with acceptance criteria (e.g., an open and fair process, as judged by the relevant authorities) can create the conditions necessary for success to be possible.

The Cloud

Question 3: Would government regulation increase confidence in cloud services and provide greater clarity on accountability and have an impact on the benefits [of] this technology?

That depends very much on the approach taken by the regulatory regime, and what it targets. Top-down 'hard' regulation is unlikely to improve any of the identified issues; co-regulation with industry input might help improve areas where it has inadequate incentives, although the incentives for providers to improve security, governance, compliance, and performance are already quite strong.

It is also not clear how regulation would improve the issues outlined. For example, technical security through regulatory requirement is notoriously ineffective in industry; current regimes are widely derided as 'tick box' exercises that do not meaningfully increase actual security.

Finally, over-regulation might harm innovation in the cloud space, which is still rapidly evolving.

Question 5: What can be done to promote competition in the cloud space rather than attempt some form of protection in this market?

There is already significant competition in the largest cloud markets (especially infrastructure-as-a-service); consumers have many choices for services like virtual CPUs and block storage. In most cases, switching costs are reasonable; an adapter or library might be needed, but because many services share base concepts, it's hard to argue that there isn't a competitive market.

This ease of switching means that interoperability mandates are unlikely to improve competition in these markets significantly. Although there are some cloud functions where switching costs are high (e.g., some platform-as-a-service offerings, and many software-as-a-service offerings), these services are rapidly evolving to meet consumer needs, and so consideration needs to be given to whether a mandate would create more harm by effectively ossifying those markets.

Of course, there are providers in some segments with significant — even dominant — market share, and they should be closely monitored for abuses of that power (e.g., tying, self-preferencing).

Data and Privacy

Question 1: What benefits would arise from introducing a legal mechanism to allow people to seek compensation for privacy breaches in Australia (e.g. establishment of a statutory tort for serious invasion of privacy)?

One of the Privacy Act 1988's greatest problems is enforcement. For example, Katharine Kemp has written about a 'forgotten privacy principle'[8] that should remove entire classes of widespread privacy abuse. Because there is no effective enforcement, it is inoperative.

A statutory tort for serious invasion of privacy would help to give the Privacy Act the teeth that it is so often missing.

Question 3: Do further changes to privacy laws in Australia need to be made to better protect Australians and change corporate attitudes regarding data collection and management?

Yes. The analogies that people use to conceptualise privacy don't fit the capabilities that are now available, and so most Australians do not fully appreciate the risks they face. The breadth of information that can be digitised and linked together is now vast; what can be inferred from it (using techniques like machine learning) is only growing. For example, widespread practices such as 'fingerprinting' exploit the 'data exhaust' of Australians to infer their personal information, even when they explicitly try to avoid tracking.[9]

Many businesses comply with their obligations to handle personal data responsibly. However, in my experience, some whose business models depend upon exploitation of personal data will only follow the letter of the law, not its spirit. Others will go further and only comply where there is a reasonable risk of enforcement — which is often small, due to the fast-moving, global, and highly technical nature of the industry. In short, some parties with access to large amounts of personal data have a significant ethics problem.

In this environment, privacy requires not only higher standards but also deeper capabilities in monitoring and enforcement.

Children's Safety

Question 1: How effective is the current legislative framework in protecting children and preventing online harm from occurring?

The eSafety Commissioner is doing an excellent job of executing the mandate given to her by legislation. However, I suspect it is too early in that execution to accurately measure effectiveness.

---

[8] Katharine Kemp, "Australia's Forgotten Privacy Principle: Why Common 'Enrichment' of Customer Data for Profiling and Targeting is Unlawful" (20 September 2022) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4224653>.

[9] See Mark Nottingham, "Not Similar to Cookies: Device and Browser Fingerprinting as Sensitive Personal Data" (16 December 2020) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3890545> for an exploration of this topic.

Effectiveness is not the only criteria which should be considered, however.

Current legislation delegates the establishment of 'industry codes' to big tech-dominated industry groups, as overseen by the eSafety commissioner. Because of the structure of the legislation, however, these codes are applicable to all Web sites, no matter what their size, nature, or who runs them. Community-oriented sites, volunteer sites, and individually-run Web pages will all be bound by these industry-created codes.

This brings two problems.

First, it will have the effect of placing a regulatory burden on all sites and services, not just the big tech companies that created the codes. Individuals and community groups that wish to avoid being trapped inside big tech platforms will be forced to comply with them, or will reduce their functionality to avoid onerous regulation. This will have anti-competitive effects as well as impacts on freedom of expression and freedom of assembly.[10]

Second, the eSafety commissioner is compelled to evaluate these proposals only in terms of online safety, with no reference to other societal goals (such as those outlined above) in establishing legislation. The process for evaluating the proposals is opaque, with little oversight or right of recourse. While the eSafety Commissioner might exercise discretion in the application of the codes to small and non-commercial services, relying upon discretion implies a democratic deficit that should be avoided.

That is not to say that the overall approach taken by Australia's online safety legislation is inappropriate; if it were limited only to 'big tech' platforms, for example, these concerns would be largely avoided. However, the current framework fails to appreciate the effects of its overly broad application.

As a result, I urge you to launch a review of the eSafety legislative framework with particular attention to how its goals are balanced with other concerns, such as freedom of expression and freedom of assembly. Online safety is an important societal goal, but it cannot be pursued without reference to others.

Question 2: What more can be done to enhance online safety for child protection in Australia?

'Big tech' companies could take a more aggressive approach to address child safety concerns — in particular by improving how child safety is implemented beyond the narrow confines of individual products. Some solutions have been proposed and seen adoption stymied by concerns by big tech companies about the effort required to implement them,[11] and regulatory pressure might change these companies' behaviours where voluntary standards failed to so do.

---

[10] See Mark Nottingham, Geoff Huston AM and Martin Thomson, "Submission Regarding the Proposed Industry Codes for the Online Safety Act 2021" (October 2022) <https://www.mnot.net/papers/22-09-esafety-industry-codes.pdf>.

[11] See, eg, Mark Nottingham, "On RFC8674, the safe preference for HTTP" (Blog Post, 5 December 2019) <https://www.mnot.net/blog/2019/12/05/safe_hint>.

Any such regulatory effort will need to consider appropriate use of power not only regarding online safety, but other concerns — including both rights like those outlined above and the continued success of the Internet.[12]

The Metaverse

Question 1: Given the currently ambiguous status of the Metaverse and its development, is it necessary to begin regulating it now, or should authorities wait in order to understand better how it will function?

I have many doubts about the viability and value of the 'metaverse', but I will put those aside to make some general observations.

First, one can consider some aspects of the metaverse as infrastructure, much as (for example) the Internet and the World Wide Web are. That infrastructure embodies a form of regulatory power, because it defines what is and is not possible to do when using it. That power should be scrutinised for who it accrues to and what abuses it allows. The best time to do that is when it is still being designed rather than after the fact, since making incompatible changes to technical architectures at scale is notably difficult.

Second, the applications 'on top' — e.g., videoconferencing, social networking, gaming -- should be scrutinised and regulated separately, as need be. Just as with the Internet and the Web, some applications will require special handling, while others will be safely ignored; likewise, the associated harms may take some time to emerge (although similarities with some existing applications can be drawn and acted upon).

It is worth noting that many abuses by applications can be controlled without legal intervention by an infrastructure that is designed to prevent them; or they can be exacerbated by one that doesn't.

Question 2: What regulatory frameworks are required both internationally and in individual jurisdictions to address the risks associated with the Metaverse?

Specifically addressing the 'infrastructure' aspect, I note the metaverse appears to be completely driven by commercial concerns at this point. In contrast, both the Internet and the Web had considerable non-commercial (e.g., government, academic, and civil society) participation in their formative stages, which continues to this day.

This is a marked difference. Whereas an argument can be made that both the Internet and the Web were created as global public goods (per Tim Berners-Lee, 'this is for everyone'), that argument cannot be made for existing iterations of the

[12] See, eg, Michael Kende et al, "Study on the Internet's Technical Success Factors" (December 2021) <https://blog.apnic.net/wp-content/uploads/2021/12/MKGRA669-Report-for-APNIC-LACNIC-V3.pdf>.

metaverse; they are commercial confections designed to benefit their controllers, not society.[13]

In particular, the current metaverse proposals do not have the concept of a 'user agent' — a component charged with representing the interests of the end user when they interact with others. In the Web architecture, the browser fills this role, and while there are still significant problems on the Web, this separation of concerns has prevented many abuses.[14]

Absent responsible self-regulation, other regulatory forces will need to be deployed, especially if the metaverse emerges as an important global infrastructure.

This leaves governments with an unfortunate choice; if regulation is imposed now, it may be wasteful if the metaverse does not eventuate as an important platform. If it does become one and sufficient regulation is not imposed, the abuses enabled could far surpass those seen on top of the Internet and the Web, because the infrastructure itself would be more amenable to that abuse, so long as it was aligned with the interests of those who control it.

Given that conundrum, a reasonable strategy might be to clearly communicate to industry that metaverse infrastructure that is not designed under open, public conditions with a broad selection of stakeholders will be more likely subjected to strong regulation.

Question 3: How would any regulatory frameworks encompassing the Metaverse be enforced?

As outlined above, interoperability mandates based upon specifications developed in the open and with the contributions of a variety of stakeholders are most likely to result in infrastructure that meets societal goals, rather than just the goals of the companies who build it.

International

Question 1: How can Australia best approach regulating the increasing number of foreign owned tech companies that have established themselves in Australia?

Running an online service in a manner that economically satisfies business requirements for availability, functionality, and support requires significant scale, and results in a tendency to have relatively few global 'winners' in each segment of the market, and a corresponding flood of overseas operators into the Australian market (which is, after all, relatively small).

Reasonable companies will be concerned about marginal costs associated with regulation, not the imposition of regulation itself. Therefore, coordination of

---

[13] See also Janna Anderson and Lee Rainie, "The metaverse will not fully emerge in the way today's advocates hope", Pew Research Center (30 June 2022) <https://www.pewresearch.org/internet/2022/06/30/the-metaverse-will-not-fully-emerge-in-the-way-todays-advocates-hope/>.

[14] See Robin Berjon, "The Fiduciary Duties of User Agents" (15 April 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827421>.

regulation across jurisdictions is most likely to result in positive outcomes and buy-in from those subjects to regulation.

Question 2: How should western democracies approach the data collection activities of companies based in countries whose political systems are more authoritarian and who may demand access to said data?

Closing the loophole in section 6A(4) of the Privacy Act 1988 would be a good start; while it is necessary for Australian privacy law to harmonise with foreign legal regimes, it should not be unconditional.

This implies that Australia might need to create an adequacy regime similar to the GDPR's. While the Privacy Act Review contemplates such a scheme,[15] its focus is on commercial entities (through APP 8). To address these concerns, it will also need to consider how foreign governments handle private information — in particular, the privacy measures embedded in national security legislation.

In doing so, we should also consider the corresponding measures in the Privacy Act. If Australia wishes to obtain GDPR adequacy, we should reconsider whether the national security exceptions in our legislative framework (including the Privacy Act) will withstand scrutiny, lest Australia be the target of another series of *Schrems* actions.[16]

Also of concern are overseas services that have no Australian presence to target for enforcement. While the urge to block such services is understandable, it should be resisted — that is the act of an authoritarian regime, not an open democracy.

Instead, the most practical path forward is to educate Australians about these risks and to provide information services (e.g., about how particular extra-territorial services might use your data).

Big Tech disinformation

Question 3: Does the former government's Social Media (Anti-Trolling) Bill 2022 adequately address online safety and, if so, should it be reintroduced to the Parliament?

No, and definitely not. Defamation law in Australia desperately needs reform, but by creating a problematic complaints scheme and casting it as an online safety mechanism that even the eSafety Commissioner distanced herself from.[17]

---

[15] Attorney-General (Cth), 'Privacy Act Review' (Report, 2022), 237.

[16] For an exploration of some of these issues, see Mark Nottingham, 'Applying the European Essential Guarantees to ASIO Computer access warrants: Can Australia avoid the trade impact of Schrems II? ' (Paper, 30 September 2021) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3933661>.

[17] Julie Inman Grant, "Opening Statement: Inquiry into the Social Media (Anti-Trolling) Bill 2022" (10 March 2022) <https://www.esafety.gov.au/newsroom/media-releases/opening-statement-inquiry-social-media-anti-trolling-bill-2022>.