Submission

Regarding the Proposed Industry Codes for the Online Safety Act 2021

Mark Nottingham mnot@mnot.net
Geoff Huston gih@apnic.net
Martin Thomson mt@lowentropy.net

Introduction 1

Applying the Codes as Written 2

Unwelcome Effects 4

Harm to the Internet 4

Impact on Freedoms of Expression and Assembly 4

Impact on Competition 5

Recommendations 5

Social Media Services 5

Relevant Electronic Services 6

Designated Internet Services 7

Equipment 7

About the Authors 8

Thank you for the opportunity to comment on the proposed Industry Codes.

We recognise that online safety is an important goal that requires regulatory oversight of industry, and that industry involvement in the formation of regulation helps to assure its success. However, we have concerns that as written, these proposed Industry Codes are harmful to the Internet itself, would have serious impacts on freedom of expression and freedom of assembly on the Australian Internet, and furthermore may have anti-competitive effects.

If adopted, we are concerned that the Codes will the effect of handing control of the Australian Internet over to the biggest of technology enterprises, endangering both the economic health of this country and the basic societal tenets of what it means to be a healthy democracy in today's world.

In this submission, we detail our concerns and recommend changes to the proposed Codes that we believe will mitigate those risks.

Introduction

Much of Australian online discourse and content flows through publication and editorial channels operated by 'big tech' companies, and we agree that those platforms have a responsibility to govern themselves and the content that they promulgate in a manner that is

compliant with legal regulation, including the Online Safety Act 2021 and any Industry Codes that the eSafety Commissioner registers.

However, those companies do not create or fully encompass 'the Internet' in terms of content and online behaviours. Our issue with the proposed Industry Codes is that they propose a regulatory regime that applies requirements designed for 'big tech' organisations to private Australians' online activities outside those platforms. While the Codes make some attempts to scale the burden of their application, the tiers as defined also encompass the operation of individual and small-scale community online sites and services with low risk for online safety issues. Because the Internet is much more diverse than suggested by the Codes, we believe this over-capture will have a disproportionately negative effect on those services without providing any commensurate improvement in online safety.

Applying the Codes as Written

These unwelcome effects can be illustrated by applying the codes to some common examples.

The Act states that Industry Codes apply to anyone who is 'a person [who] is a member of a group that constitutes a section of the online industry.'[1] As the FAQ affirms, this means that (inter alia) "the codes will be mandatory for all websites and apps available in Australia, which are considered to be 'designated internet services.'"[2]

The Designated Internet Services Online Safety Code proposes that some sites be exempt from risk assessment (and effectively, exempt from the code):

> A provider of a designated internet service is deemed to be a Tier 3 service and not required to conduct a risk assessment where: (i) the designated internet service is a general purpose website or app or a classified DIS.[.][3]

However, 'general purpose website' is narrowly defined using a closed list:

> [G]eneral purpose website or app means a designated internet service that primarily provides information for business, commerce, charitable, professional, health, reporting news, scientific, educational, academic research, government, public service or emergency service purposes and/or enables related transactions.[4]

… while a 'classified DIS' adds 'general entertainment, news, or educational content' with certain conditions.[5]

Because the exemption is scoped using a closed list, many sites and content sources would be subject to this regulation, even though the risk that they represent to online safety is minimal.

---

[1] *Online Safety Act 2021* (Cth), s 136.
[2] 'Frequently Asked Questions' (Web Page) <https://onlinesafety.org.au>.
[3] 'Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)' (1 September 2022), s 4(d) ('Designated Services Code').
[4] Designated Services Code (n 3), s 3.
[5] Ibid.

For example, a purely personal Web site (e.g., a blog) does not clearly qualify for exemption. Neither does a community group, a site for a shared interest or hobby, an online tool, or even a joke site. All are common on the Internet.

Furthermore, because the definitions of each kind of site qualifying for exemption are open to interpretation, application of any such exemption is not likely to be consistent, and the resulting doubt is likely to create a strong chilling effect on independent online publication.

For example, does a site about health issues qualify as 'health', or does one need to be registered with a recognised health-related authority to qualify? Is my personal site considered 'professional' because I talk about mostly professional things on it, or does it need to be associated with an ABN? Will 'academic research' only be considered such when its online publication occurs via an .edu.au domain name?

These overly broad effects are not limited to Designated Internet Services. The Social Media Services Online Safety Code excludes from Tier 3 *any* online service with messaging, chat services, image sharing, or user profiles.[6] That means that local community discussion forums[7] will need to undertake expensive compliance efforts, both up front and on an ongoing basis. So will any community or social group that wants to use a Web message board, online forum, MUD or MOO. They will necessarily need apply comprehensive measures to identify all contributors, hold the resulting personal information in a robustly secure manner, and obtain expert advice regarding their responsibilities and liabilities in operating such a community forum. This imposes a significant burden on such community and social groups that seems to be significantly greater than the commensurate level of risk posed by these activities.

Similarly, the Equipment Online Safety Code requires a provider of an Operating System to

> take part in an annual forum organised and facilitated by one of the industry associations responsible for the development of this Code […] to discuss and share relevant issues, advances and best practice in online safety with other industry participants.[8]

and:

> An OS provider must take reasonable steps to develop and implement tools within operating systems that allow Australian end-users to help reduce the risk of harm to children when using interactive (Tier 1) devices.[9]

These requirements fail to recognise that some Operating Systems are community-led (e.g., Linux, FreeBSD) with active Australian participants, but do not have the same capacity that multi-billion (or even trillion) dollar corporations do.

---

[6] 'Schedule 1 – Social Media Services Online Safety Code (Class 1A and Class 1B Material)' (1 September 2022), s 3(d) ('Social Media Code').
[7] See, eg, 'whirlpool' (Web Site) <https://whirlpool.net.au>.
[8] 'Schedule 8 – Equipment Online Safety Code (Class 1A and Class 1B Material' (1 September 2022), s 7.
[9] Ibid.

Unwelcome Effects

If adopted, the Industry Codes will have several undesirable effects on the Australian Internet and those who use it.

Harm to the Internet

A key architectural property of the Internet is *permissionless innovation* – the ability to add new kinds of services without significant barriers to entry.[10] Permissionless innovation is the engine of the Internet's success; without it, Australian society would not enjoy the benefits to quality of life, commerce, and society that we do today.

In large part, that is because many (if not most) of the Internet services that we enjoy today started as small personal projects or were directly inspired by them. Often, large, centralised Internet services are nothing but the re-packaging of what had previously been distributed and ad hoc (see, e.g., RSS feeds).

A requirement that most new services on the Internet undertake a regulatory risk assessment and other compliance activities would create such a barrier. In turn, we would expect the Australian Internet to be less diverse, less representative of broader society, more commercial, and more concentrated as a result. It would be less the Internet as we know it, and more of a 'walled garden' – keeping in mind that the Internet already faces considerable pressure towards consolidation of power by large companies (see also 'Impact on Competition' below).

Impact on Freedoms of Expression and Assembly

Although much of online discourse and content flows through 'big tech' companies, it is still not uncommon for people to create self-hosted discussion boards, blogs, personal sites, interest-based sites, and so on.

Requiring students, parents, teachers, community groups, social groups, interest groups, and other non-commercial bodies who wish to create a Web site to undertake the same compliance activities as multi-billion (or trillion-) dollar companies is not proportional or equitable, and has significant impact upon their freedom of expression, the freedom of expression of their users, and freedom of assembly for all.

Requiring the diverse community of Open-Source Operating System contributors to live up to the same regulatory requirements within Australia as the largest companies in the world is likewise stifling their freedom of expression, and since Open-Source communities lie at the foundation of the digital economy and the measures being contemplated here would push much this activity out of Australia.

Even if the Commissioner were to exercise judgement in applying the Codes, the need to rely on that discretion would have a chilling effect on open expression and assembly. By 'herding'

[10] See, eg, Leslie Daigle, 'Permissionless Innovation – Openness, not Anarchy', *Internet Society* (Blog Post, 22 April 2014) <https://www.internetsociety.org/blog/2014/04/permissionless-innovation-openness-not-anarchy/>.

discourse to a small number of platforms who are capable of being compliant, diversity of Australian expression and assembly will suffer, and our society will progress further along a path that would be the antithesis of a free and open democracy.

Impact on Competition

Small businesses, community groups and individuals already face significant technical and practical barriers to hosting their own Web sites and online services; many have chosen to only be present on large, proprietary platforms as a result.

Much attention has been paid to the concentration of power into digital platforms, as well as potential abuses of that power. Finding effective remedies has proven challenging, whether they be technical or legal responses, in part because the platforms have been so successful in limiting market entry by new undertakings – commercial or otherwise. In such an environment, any disincentive or barrier to the use of alternative approaches creates even more momentum for the takeover of the entire digital environment by the global online giants.

With this in mind, it is difficult to see industry-led regulation that adds a considerable compliance burden to those who wish to avoid large, proprietary platforms as anything but anti-competitive.

By precluding an important source of substitution – the consumers' ability to provide a service themselves – the proposed Industry Codes can be seen as an arrangement that is likely to have the effect of controlling or maintaining the prices of services that are provided by many of the authors of the Codes.[11]

Recommendations

The eSafety Commissioner has a variety of tools at their disposal. We do not propose that small, non-commercial Web sites and online services be exempt from regulation, or that unsafe activities on them be ignored or tolerated; only that regulatory tools designed and sized for large businesses not be applied to them.

In particular, we observe that smaller, more cohesive communities – whether they be collected around a neighbourhood, a friend grouping, a family, a common interest, or a common background – tend to be more self-regulating than the artificial and very large 'communities' on commercial social networks and similar services.

Social Media Services

The Social Medial Services Online Safety Code applies to any service whose primary purpose is 'online social interaction' that 'allows end-users to post material on the service.'[12] With such a broad definition, this Code is likely to include any online gathering place in Australia – even ad hoc, non-commercial ones.

The proposed Code does exempt Tier 3 services, but such services cannot 'create a list of end-users with whom an individual shares a connection with…', 'view and navigate a list of

[11] See *Competition and Consumer Act 2010* (Cth), s 45AD.
[12] Social Media Code (n 6), s 2.1(c)(i)(C).

other end-user's individual connections', or 'construct a public or semi-public profile within the bounded system created by the service.'[13]

These restrictions are problematic. By hobbling small, community gathering places – for example, locally-hosted message boards – by denying fundamental features, these industry-led constraints appear to be forcing more content and discourse onto big tech platforms. Australians will effectively be required to communicate using those (often, overseas-owned) platforms.

For example, if someone wanted to set up a message board for their neighbourhood or for people who hold similar interests, they can currently do so using any one of a variety of Open-Source tools.[14] Requiring these communities to undertake compliance activities (and the associated risks) is not reasonable; as stated above, they are typically much better at self-policing than large tech platforms, and when a problem is found, the Commissioner still has many tools at their disposal.

These effects can be mitigated by removing 3(d)(iii). If the Commissioner feels that is too broad, an additional requirement that the service be non-commercial could be added.

Also, if industry and the Commissioner were to give meaningful support to non-commercial and small services regarding their compliance requirements – for example, guides, tools, advice, help desks, Open-Source software to support certain functions (provided it wasn't used as a backdoor to collect more data), that might also assist this sector in maintaining their online presence. However, any requirement on smaller services should not be imposed until such support is available for a service's chosen tools, and of high quality.

In either case, public services not provided by any one entity (for example, Usenet) that are based upon widely recognised technical standards should be explicitly exempted, to remove any doubt about how they should be handled by other parties. While such services are not free from problematic content (by any means), applying Industry Codes to them is inappropriate and unlikely to lead to better safety outcomes. Their regulation should be considered separately.

Relevant Electronic Services

Like Social Media Services, the Relevant Electronic Services Online Safety Code predicates qualification for Tier 3 (and thus exemption) on not allowing 'end-users to view a list of other users' individual connections', 'search for other end-users […] using known identifiers', 'search for other end-users […] based on interests or keywords', and 'recommend[ing] other contacts […] based on interests or shared connections.'[15]

---

[13] Ibid, s 3(d).

[14] See, eg, Rajkumar Maurya, '11 Best Open source Forum Software for Free Online Discussion', *H2S Media* (Blog Post, 6 January 2022) <https://www.how2shout.com/tools/free-best-open-source-forum-software-online-discussion.html>.

[15] 'Schedule 2 – Relevant Electronic Services Online Safety Code (Class 1A and Class 1B Material)' (1 September 2022), s 6(c).

Again, this is too broad; messaging is a fundamental activity on the Internet, and identity (and thus profiles) are intrinsic to it. Tying a large compliance burden to these functions effectively hobbles many potential Internet services and drives more traffic to 'big tech' platforms.

These concerns could be addressed by removing, in 6(c), the box at the intersection of 'Tier 3 Indicators' and 'Discoverability of users.' As with social media services, an alternative approach might be to provide adequate support.

And, as with Social Media Services, public services not provided by any one entity (for example, IRC, Matrix and Mastodon) that are based upon widely recognised technical standards should be explicitly exempted.

Designated Internet Services

The Designated Internet Services Online Safety Code nominates types of Web sites for exemption based on a closed list. This is problematic for the reasons discussed above. Adding new types of sites to the list is not appropriate, because there is not a closed list of things you can do on the Internet.

It also disqualifies any site that allows 'end-users to upload content'.[16] This is unworkable, since 'content' is such a broad concept. Sites that allow chat or messaging are similarly disqualified, despite the arguments regarding those functions above.

As a result, 4(d) needs to be completely reworked. Placing an industry-focused compliance burden on most every Web site in Australia is clearly undesirable, disproportionate, and will lead to Australian online discourse and content being concentrated into a few, powerful hands. In almost every case, it's also unlikely to lead to meaningful improvements in online safety.

We suggest that instead of focusing on types of sites or features they use, a good starting point would be whether they are commercial in nature and assessing their level of social impact and visibility as a baseline for inclusion in these codes. For example, id.au domains[17] should not require compliance to industry codes, nor should similar sites in other top-level domains.

Equipment

The Equipment Online Safety Code currently tiers its application by degree of user interactivity. While this is one important metric, it also captures significant hobbyist and Open-Source community members.

Requiring compliance from these participants is not proportional. It is also not effective; because most projects have at least some overseas contributors, the regulatory burden inherent in the proposed Code creates a disincentive for Australian participation and innovation, rather than leading to safer outcomes.

---

[16] 'Schedule 3 – Designated Internet Services Online Safety Code (Class 1A and Class 1B Material)' (1 September 2022), 4(d)(ii).

[17] See 'id.au rules – eligibility and allocation', *.auDA* (Web Page) <https://www.auda.org.au/au-domain-names/domain-name-help/idau-rules-eligibility-and-allocation>.

One way to mitigate this over-regulation would be to have the Code only apply to equipment and Operating Systems that are commercially available in Australia, explicitly exempting non-profit, community-based and hobbyist efforts.

About the Authors

Mark Nottingham has served on the Internet Architecture Board and the W3C Technical Architecture Group, the peak architectural bodies for the Internet and the Web respectively.

Currently a member of the W3C Board of Directors and chair of the IETF HTTP Working Group for more than fifteen years, he has contributed to numerous technical standards for the Internet and Web.

Mark lives in Prahran, Victoria.

Geoff Huston AM is the Chief Scientist at the Asia Pacific Network Information Centre (APNIC), where he undertakes research on topics associated with Internet infrastructure, IP technologies, and address distribution policies.

Geoff has served in a number of roles, including as a member of the Internet Architecture Board, the chair of the Board of Trustees of the Internet Society. He has presented at a number of global technical and government forums, including the Organisation for Economic Co-operation and Development (OECD), the International Telecommunications Union (ITU), the Internet Corporation for Assigned Names and Numbers (ICANN), the Asia-Pacific Economic Cooperation (APEC), and the Internet Engineering Task Force (IETF).

In 2020, Geoff was made a member in the general division of the Order of Australia (AM) for his role as an Internet pioneer in Australia.

Martin Thomson is a Distinguished Engineer at Mozilla, based in Sydney. He is a former member of the Internet Architecture Board, and authored the technical specifications for HTTP/2 and QUIC.