Queensland University of Technology
Digital Media Research Centre

Creative Industries Precinct, Musk Avenue
Kelvin Grove Qld 4059 Australia
Phone +61 7 3138 3556 Fax +61 7 3138 3723
Email dmrc@qut.edu.au
www.qut.edu.au/research/dmrc

Department of Infrastructure, Transport,
Regional Development and Communications

By email: OnlineSafety@infrastructure.gov.au

14 February 2021

QUT Digital Media Research Centre submission in response to the draft *Online Safety Bill 2020*

Prepared by Prof. Nicolas Suzor.

About the DMRC: The DMRC is a global leader in digital humanities and social science research with a focus on communication, media, and the law. [redacted]

Introduction

It is worth noting at the outset that around the world administrative content takedown regimes are still exceptional. The examples cited in the Discussion Paper (pg. 15) from France and Germany are highly controversial.[1] Indeed, the French requirement to remove hate speech was mostly rendered invalid by the Constitutional Council in June 2020, on the basis that it impermissibly interfered with freedom of expression. Across the European Union, similar regimes refer hate speech and violent content to the digital platforms, leaving them to consider the content removal (largely according to their own platform policies), though even such regimes remain riddled with accountability issues.[2]

Remove 'offensive' from the definition of adult cyber-abuse

To the extent that administrative officials are empowered to compel private actors to remove speech, that power should be tightly constrained. The eSafety Commissioner has been successful at securing the voluntary compliance of the telecommunications and technology sector to date, and there is no reason to suspect this is to change. Where penalties are required to secure compliance, these should be limited to exceptional circumstances.

We suggest a definitional change to narrow the scope of content that is covered by the scheme. Particularly as applied against individual users, the definition of cyber-abuse should not mirror the overly-broad wording of s 474.17. We suggest removing 'offensive'

[1] See, e.g. Article 19, Responding to 'hate speech': Comparative overview of six EU countries (2018)
[2] See Lucie Krahulcova, Europol's Internet Referral Unit risks harming rights and feeding extremism (17 June 2016) Access Now.

from the definition in s 7, rewording the provision to “menacing or harassing in all the circumstances”.

Adequate exceptions are required

Any power to remove material should include clear and certain exceptions for content in the public interest. A simple example can be found in the *Abhorrent Violent Material Act*: images that are clearly in the public interest, like the notorious Abu Grhaib images, fall within the definition of AVM (depictions of torture, taken by those responsible). Clearly the *AVM Act* was not designed to criminalise the distribution of images such as these, but it does not contain sufficient safeguards to clearly create an exception. Any new legislation should avoid repeating this mistake and introduce a clear ‘public interest’ exception.

Overlap with Abhorrent Violent Material scheme

The draft Bill is in part designed to simplify existing Australian content regulation regimes. The ongoing maintenance of criminal penalties under the *Abhorrent Violent Material* provisions is incongruous with this goal. The provisions of the *AVM Act* require service providers to remove content that is covered by this draft Bill; there is no reason to maintain two takedown provisions for this material. The penalties in the *AVM Act* are disproportionate and its safeguards are inadequate; now would be a good time to repeal the *AVM Act* if a new takedown power is created.

The definition of AVM is already sufficiently broad and should not be expanded in this draft Bill to also include material that ‘promotes’, ‘incites’, or ‘instructs’ in ‘abhorrent violent conduct’. Subsection 99(3), which removes the requirement of procedural fairness, should be removed; if it is necessary to make an initial determination that is not procedurally fair, that decision should be revisited and properly made after the initial urgency has passed.

Application to infrastructure providers

Blocking content at the infrastructure level often results in unavoidably blocking a great deal of legitimate content. This is particularly the case when a service provider does not have the ability to identify and control individual pieces of content. Providers of cloud storage services, virtual private servers, and end-to-end encrypted services, for example, will often not be able to remove discrete pieces of content on their network without disabling access to entire accounts or services. The security of vital internet communications often depends on ensuring that unauthorised people — including the operators of internet services — do not have access to unencrypted content. In these cases, compliance with a removal notice should not require the service provider to suspend access to the service or terminate a user’s account. We recommend that a service provider’s non-compliance for this reason does not trigger a civil penalty. If this type of infrastructure-level blocking is required as a last resort, it should require the Commissioner to ensure that the blocking is proportionate in all the circumstances, and a clear avenue of appeal should be provided not only to the provider and user who posted the material but to anyone impacted by the block.

For similar reasons, blocking by ISPs under Part 8 should require the ISPs to redirect viewers to a page explaining the reasons for the block, and any impacted person should have a right of review to the AAT. Any extension beyond the immediate period of a crisis (measured in days, not months) should only be possible upon application to the Federal Court.

Power to identify users should be removed or tightly constrained

There is no legitimate justification for providing the Commissioner the power to require service providers to disclose personally identifying information about their users (s 194). The approach this Bill has taken is to focus enforcement obligations on service providers; removing content is easily handled by the other powers available. If a person needs to be identified because of material they have posted, this should be limited to strong prima facie cases of civil or criminal wrongdoing. In civil cases, normal preliminary discovery is available, supervised by an appropriate court. In criminal cases, law enforcement agencies already have other mechanisms of investigation. Section 194 should be removed. If it is not removed, the power to compel identification should be available only on application to the Federal Court. The provision should also note that a service provider is under no obligation to weaken encryption or design their systems to collect additional information.

Power to require enforcement of terms of service and suspend or terminate accounts

We are deeply concerned about additional tools that would empower the eSafety Commissioner to require service providers to 'enforce their terms of service', including potentially restricting or terminating service accounts. The range of enforcement options available to the Commissioner are extensive in this Bill, and there is no clear justification for this additional power. We recommend it be removed.

The cyber-abuse scheme should target 'conduct' in addition to 'material'

Technologically-facilitated abuse is not limited to discrete harmful posts. In order to adequately address bullying and abuse, the eSafety Commissioner should be explicitly empowered to investigate claims of abusive conduct (including stalking and coded threats, for example) that is not limited to individual pieces of material. The definition in Section 7 already makes reference to evaluating material 'in all the circumstances', but we suggest that the definition should explicitly extend to abusive conduct.

The cyber-abuse scheme should modify the requirement for intent

We suggest that the intent element be removed from the definition of 'cyber abuse material' in sub-section 7(1)(b). Intention should be relevant to the components of the Bill that introduce penalties for abusive behaviour, but intent is not relevant to a requirement that a service provider remove material that is likely to be harmful.

Class 1 and 2 material

Adults should not be prevented from seeking and accessing, in private, material that is not unlawful to possess. While a mandatory Restricted Access System might be justified to protect children and unsuspecting adults, the ongoing prohibition on hosting either Class 1 or Class 2 material is an unjustifiable interference with the right of freedom of expression, which includes the right to seek and receive information of all kinds.

At any rate, Section 115 should be removed from the draft Bill. The correct remedy for Class 2 material is to require the use of a Restricted Access System. There is no evidence to support any need to prohibit the availability of Class 2 material that is protected by a Restricted Access System.

Federal Court orders must be proportionate

The enforcement mechanisms in Division 9 should explicitly require the Federal Court to have regard to the proportionality of remedies sought in all the circumstances.