Communication to

Australian Government

Department of Infrastructure

Online Safety Act

Statutory Review of the Online Safety Act

Submitted for consideration

by, Radha Stirling, founder of Due Process International

Introduction

The Australian Government has requested public consultation in respect of eSafety. The issues raised have been answered below by Radha Stirling, expert witness and founder of Due Process International:

Part 2 – Australia's regulatory approach to online services, systems and processes

1. **Are the current objects of the Act to improve and promote online safety for Australians sufficient or should they be expanded?**

The scope of the Act does not require expansion. It is already so expansive with vague language such as "harmful" that it is potentially subject to misuse and abuse, depending on the political climate or issue at the time.

2. **Does the Act capture and define the right sections of the online industry?**

The Act captures literally everything online.

3. **Does the Act regulate things (such as tools or services) that do not need to be regulated, or fail to regulate things that should be regulated?**

The Act covers everything that is already subject to pre-existing laws and needs no further government regulation. The Act should certainly not regulate overseas companies or individuals who happen to have a website.

4. **Should the Act have strengthened and enforceable Basic Online Safety Expectations?**

No, pre-existing laws already cover criminal activity.

5. **Should the Act provide greater flexibility around industry codes, including who can draft codes and the harms that can be addressed? How can the codes drafting process be improved?**

"Flexibility" can be misused in the future as new regulatory bodies are established. If in the future, there is a perceived need for a new body or code, this should be tabled independently of this Act, rather than allowing the flexibility in advance which will ultimately lead to a situation where there is no public consultation on issues.

6. **To what extent should online safety be managed through a service providers' terms of use?**

External service providers should not be required to manage Australia's "online safety" demands proactively. We do not want a situation where global companies and individuals are required to comply with any country's wish lists. People should be able to decide what websites they wish to visit, whether they comply with the Australian government's desires or not.

7. **Should regulatory obligations depend on a service providers' risk or reach?**

No, this is discriminatory and vague. It's open to abuse and therefore should not be considered.

<u>Part 3 – Protecting those who have experienced or encountered online harms</u>

1. **Are the thresholds that are set for each complaints scheme appropriate?**

No, they are far too broad and conflict with the UN Declaration of Human Rights, specifically related to Freedom of Expression. The scope would allow for content to be removed and for platforms to be fined in respect to non-criminal activity.

2. **Are the complaints schemes accessible, easy to understand and effective for complainants?**

It appears that anyone who is offended can make a complaint and claim they are being targeted or that it is impacting their lives or businesses. It appears action can be taken even where that activity is lawful. That makes it extremely unfair, vague and open to abuse by complainants and the Commissioner.

3. **Does more need to be done to make sure vulnerable Australians at the highest risk of abuse have access to corrective action through the Act?**

Absolutely not. Severe cases can be taken up with law enforcement under pre-existing harassment laws which can then result in a legal order to remove content. This is not the role of an eSafety Commission.

4. **Does the Commissioner have the right powers to address access to violent pornography?**

It is already sufficiently enabled to control violent and child pornography as are law enforcement bodies. Although using the example of "child pornography" which most people find abhorrent, any proposed expansion of powers will cover other more disputed areas of issue like discrimination.

5. **What role should the Act play in helping to restrict children's access to age inappropriate content (including through the application of age assurance)?**

None. The government has no parental responsibility. This is a social issue that should be dealt with through education and the promotion of 'wholesome' values.

6. **Does the Commissioner have sufficient powers to address social media posts that boast about crimes or is something more needed?**

If "boasting about crimes" is unlawful, this should be dealt with by law enforcement. If it is not unlawful, it should not default to become unlawful via an eSafety Commissioner.

7. **Should the Act empower 'bystanders', or members of the general public who may not be directly affected by illegal or seriously harmful material, to report this material to the Commissioner?**

No, this will cause an inundation of politically and socially motivated reports. Notifying the Commissioner will become a standard part of social activism. There are already enough lobbyist groups, bot farms and governments who mass report posts they don't like to social platforms, risking violating the UN right to freedom of expression.

8. **Does the Commissioner have sufficient powers to address harmful material that depicts abhorrent violent conduct? Other than blocking access, what measures could eSafety take to reduce access to this material?**

This does not need expansion but in fact, needs more clarification. Violent abhorrent conduct is legal as depicted in Hollywood movies. Restricting "violent" content can impact on the public's ability to protest or share true (or made up) information. Recommending the public make responsible decisions is the best solution.

9. **What more could be done to promote the safety of Australians online, including through research, educational resources and awareness raising?**

Further education in respect of avoiding online scams would save a lot of people a lot of money. As far as safety is concerned, people need to understand that they can block people or websites voluntarily if they don't like the content. That is the extent of the service governments should provide in online education.

<u>Part 4 – Penalties, and investigation and information gathering powers</u>

1. **Does the Act need stronger investigation, information gathering and enforcement powers?**

Definitely not. We already have law enforcement to deal with crime and do not require an additional government body that can be weaponized against people and platforms.

2. **Are Australia's penalties adequate and if not, what forms should they take?**

The penalties are disgracefully high to the point where the fines involved act as an incentive for the department to make inappropriate requests to remove content in hope the platform does not comply and they are financially rewarded.

It is completely inappropriate to fine an individual $156,500+ and jurisdictionally flawed to fine a company that doesn't even operate within Australia (as was threatened against X). No company registered outside of Australia should ever be issued with a local penalty. Universal jurisdiction is risky and frankly, unlawful. If we wouldn't accept Saudi Arabia penalising an Australian company who had a site on the world wide web, then we should not be attempting to initiate the same.

3. **What more could be done to enforce action against service providers who do not comply, especially those based overseas?**

No further “actions” should be taken against service providers who “do not comply”. Citizens can exercise their personal responsibility by choosing online content well. Education over censorship.

4. **Should the Commissioner have powers to impose sanctions such as business disruption sanctions?**

Absolutely not. The Commissioner should never be able to issue any sanctions against businesses. We are not living in a communist regime and should refrain from acting as though we are. This concept would be open to significant abuse by the Commissioner and the government.

<u>Part 5 – International approaches to address online harms</u>

1. **Should the Act incorporate any of the international approaches identified above? If so, what should this look like?**

A voluntary “suggested” and “encouraged” model is much less open to infringing on the right to freedom of expression. If a platform tends to ignore these “guidelines”, citizens can be recommended to avoid them and take their business elsewhere. This could be similar to giving a product an “organic” or “made in Australia” tick but still gives citizens the choice to buy a “lesser” product should they wish. If Australians want safe content, let a technology company develop a PG/censorship browser for their use.

2. **Should Australia place additional statutory duties on online services to make online services safer and minimise online harms?**

No. Again, we delve into issues pertaining to universal jurisdiction. If we would accept Saudi dictating the “duties” non Saudi companies have, we should not ask for it ourselves. If our friends in other countries are attempting this, we should discourage the overreach.

3. **Is the current level of transparency around decision-making by industry and the Commissioner appropriate? If not, what improvements are needed?**

If there must be a Commissioner, he or she should be an elected representative and changes to their roles, responsibilities and authority should be voted on by online referendum every single time. With instant access to be able to participate in democracy, there is no reason why these issues should not require public consultation every single time.

4. **Should there be a mechanism in place to provide researchers and eSafety with access to data? Are there other things they should be allowed access to?**

eSafety and “researchers” should not be given mechanisms to access data. Any access requests coming from eSafety should require going via law enforcement and then through a

court to obtain a warrant before they are able to be granted any information held by third parties.

If there is data held by the Commissioner, it should be made available to the public under freedom of information principles. This would enable the public to know whether the Commissioner is abusing their authority.

5. **To what extent do industry's current dispute resolution processes support Australians to have a safe online experience? Is an alternative dispute resolution mechanism such as an Ombuds scheme required? If so, how should the roles of the Ombuds and Commissioner interact?**

We already have courtrooms available to serious disputes and the concern with a binding, unelected ombudsman is that it is another government body that would likely side with the government. This could remove remedies from victims and allow unchecked government abuses. Thus, any decision by any potential Ombudsman should be appealable by the individual or company, but not by the Commissioner.

6. **Are additional safeguards needed to ensure the Act upholds fundamental human rights and supporting principles?**

In the same way that human rights provisions were (at the last minute) inserted into the UAE - Australian extradition treaty, the right to freedom of information, opinion and expression (speech) is crucial and is the most likely right to be trampled on by the eSafety Commissioner. It is this right that must be defended first.

<u>Part 6 – Regulating the online environment, technology and environmental changes</u>

1. Should the Commissioner have powers to act against content targeting groups as well as individuals? What type of content would be regulated and how would this interact with the adult cyber-abuse and cyberbullying schemes?

No, there is no need for additional powers already covered by the law and other sections of this Act.

2. **What considerations are important in balancing innovation, privacy, security, and safety?**

Privacy and safety are issues usually covered by existing harassment laws. If there is a genuine risk, a police report can be made and escalated to the appropriate platform. Social media companies already comply with law enforcement requests. The right to privacy can not be automatic and enforceable through the Commissioner as it will often conflict with the right to information and freedom of expression.

3. **Should the Act address risks raised by specific technologies or remain technology neutral? How would the introduction of a statutory duty of care or Safety by Design obligations change your response?**

Changing the Act every time new technology is introduced is going to keep people in jobs. Like a Constitution, an Act should be made for longevity but it should not be vague either. Thus, it should only cover the absolute minimum intervention required, allowing it to stand the test of time.

4. **To what extent is the Act achieving its object of improving and promoting online safety for Australians?**

The Act is providing an avenue for politically charged censorship and the expansion of governmental powers to curb UN rights to freedom of information and expression thus making Australians less safe.

5. **What features of the Act are working well, or should be expanded?**

If one is a victim of criminal harassment, they may (in theory) receive a speedier response from eSafety than from the police. However, that is at the expense of unreasonable interference in the entire population's right to freedom of expression and information. This should certainly not be expanded.

6. **Does Australia have the appropriate governance structures in place to administer Australia's online safety laws?**

Australia has already quadrupled the budget of an unelected and largely unsupported, controversial body. Until issues of censorship and free speech have been properly considered, debated and resolved, no consideration of "appropriate government structures" should be discussed.

7. **Should Australia consider introducing a cost recovery mechanism on online service providers for regulating online safety functions? If so, what could this look like?**

Absolutely not. Is eSafety simply a money making scheme for the government? A significant portion of Australians have publicly stated they would prefer eSafety to be defunded. If Australia began to see eSafety as a profit centre, the body would be more inclined to seek to expand its powers. This is not beneficial to the Australian population who may prefer a limited version of the body.