# Submission: Online Safety Bill 2020

The Online Safety Act presents several concerns which, if ignored, will turn Australia into the laughing stock of the technology industry, and will drive our technology industry overseas. A possible voluntary online safety scheme is also proposed in this submission.

## 1. A repeat of history

Sections that relate to Class 1 and Class 2 material have nothing to do with cyber-bullying, and are more to do with films and video games without classifications, and copyright legislation. This is reminiscent of an attempt that took place around 2008-2011, championed heavily by lobby groups such as the Australian Christian Lobby (ACL) to censor material for all Australians online. Elements of the proposed legislation mirror those of oppressive regimes such as China and Iran.

**All sections in Divisions 2, 3, 4, 5, 6, 7, 8, 9 and 10 (Part 9) only pertain to Class 1 and Class 2 material; they should be eliminated as this is irrelevant to cyber-safety.**

Instead, a site should produce a warning where Class 1 or Class 2 material may be present, allowing people to make informed decisions regarding access to online content. **For this purpose, Division 1 (Part 9) serves as definitions to what constitutes Class 1 and Class 2 material.**

## 2. Inadequate protection against vexatious complaints

A common method of bullying others is to accuse them of a wrong-doing, and pretend to be the victim. Such may be an individual or group, who is capable of manipulating others into being "witnesses" and providing false or misleading information.

Many people of questionable character (including scammers and extremists) have successfully used false accusations of rape, racism, sexism, or similar forms of harassment to ruin peoples' lives, and coerce victims against warning others including authorities. Such tactics are often used to stifle freedom of speech, and is often used by those who dislike the opinions of others.

Minors will often use vexatious complaints against adults (including parents and teachers) who do not cater to their demands. There is also potential for rivalling parents to use vexatious complaints against each other in a similar manner to that described above.

The Government must be careful not to enable these scrupulous people. There are some "good faith" tests present in the proposed legislation, however these offer insufficient protection against a well-resourced cry-bully.

**The proposed legislation should make vexatious complaints a criminal offence, punishable by fines, prison terms, or refusal of investigation into future complaints for a period of time.**

**Provisions of self-defence should also be included to allow for an individual protecting themselves and others from vexatious persons.**

# 3. Jurisdiction and scope creep

No act of an Australian parliament has standing in any country other than Australia. Australian victims of international cyber-abuse will have no recourse with the Australian legal system.

The government must also ensure the scope be limited exclusively to social media platforms, and exclude small forums or other online communities.

**There are currently no clear definitions within the Basic Online Safety Expectations (Part 4) that excludes smaller online social communities from this legislation.**

**It is also not possible for sites that operate overseas to be required by Australian legislation to prevent access to Class 1 or Class 2 material.**

### *3(a). Commercial Interest Test*

It is worth limiting the scope by applying a "commercial interest test" to social media services, relevant electronic services and designated internet services. Such a test may determine whether there is significant income obtained from the use of that service, including, but not limited to, advertising regimes and internal "currencies" such as in-game points or other tokens.

# 4. Insufficient use of existing resources

This legislation is completely unnecessary in the context of a variety of resources that we have in place already. This includes both government and private resources.

The Australian Government has an extensive law-enforcement portfolio, which includes state and federal police, who work with international organisations such as INTERPOL. These agencies are capable of using existing resources against cyber-bullies without needing new legislation.

### *4(a). Private sector resources available*

The fact sheet for the bill[1] states the following:

> "However, experience has shown that many platforms lack the built in safety features required, or fail to appropriately enforce their terms of service."

This is misleading; many social networks are vigilant about the content they allow on their sites. It is within the best interests of service providers to have reasonable moderation policies. Such policies are often enforced by their moderation staff, without requiring government intervention. In fact, voluntary cooperation with law enforcement agencies is not uncommon.

To continue this level of co-operation, the Government must maintain a good working relationship with online communities. The reporting requirements proposed in the bill may damage this relationship, as it paints the image of the Government being an enemy to public discourse.

There should be no non-voluntary mandatory reporting requirements unless ordered by federal or state courts; **Division 3 (Part 1) should be removed or reviewed.** Instead, a scheme is proposed in this submission to allow the Government to maintain a good relationship with the private sector, essential for resource sharing and co-operation.

# 5. Concerns of excessive powers

The Government must take care not to place Australia at risk of losing standing with international allies who favour freedom of expression and freedom of speech.

**Division 3 (Part 4), Subdivision C renders innocent people at risk of exposure.** This should be managed by a court of law instead.

**The sections allowing the eSafety Commissioner to require a person to provide their personal information (all of Part 13) must be removed, as this denies the person the right to a fair trial.** The function of the Federal Court and Federal Circuit Court are acknowledged as per Part 10.

**All of Part 14 must be eliminated, as it presents an extra-judicial proceeding, contrary to what is available in a fair trial by a court of law.** However, **Section 204 (*Protection of persons giving evidence*) is agreeable.** Australian courts are already able to compel people to provide evidence, and as such, this renders Part 14 redundant and unnecessary.

**If the eSafety Commissioner wishes to investigate someone, he/she must have probable cause and it must be related to a complaint.**

# 6. Proposal: voluntary registration scheme

The Government's relationship with the private sector is an essential economic and national security tool. The reporting scheme in Division 3 (Part 1) is potentially damages such relationships.

**A viable alternative to Division 3 (Part 1)** is a framework that allows staff of service providers (such as moderators and administrators of social media services) to co-operate voluntarily, which many are willing to do. Such a scheme could involve the following:

1. A lframework which allows service providers, site owners, or other relevant personnel to voluntarily register themselves as being safe from cyber-bullying. **Such a service may wish to display a logo or icon which denotes their participation in such a scheme.**
    - Similarly to above, a voluntary scheme for services which also emphasise safety for children.
    - Provisions for "hybrid" services, which may provide access controls for adult content.
2. Instruments which allow service providers to report suspicious or harmful content to authorities. Many service providers are willing to co-operate if assured that they will not be prosecuted.
    - This should apply regardless of whether or not the site is voluntarily registered as per above.
    - Such material should be presentable as evidence in an Australian court of law.
3. Encouragement from Government agencies to make service providers to make sites aware of these initiatives. This may include a publicly-accessible list maintained by a Government agency.
    - Such a scheme may include incentives for search engines to prioritise sites that have voluntarily registered. For instance, Google has a "Safe Search" function which allows for a family-friendly search experience.

# 7. Inadequate time frames

The proposed legislation often provides very short time frames of 24 or 48 hours; this may not be sufficient for response times within smaller service providers.

It is recommended that this be increased to 72 or 96 hours for smaller service providers, or at least this time frame be determined on a case-by-case basis depending on the size of the service provider, the level of exposure they present, and the staff that are employed there.

Furthermore, such material may be available on Internet archives long after it is removed from the original service provider.

# 8. Home-grown terrorist threats

One of the motivations behind the new blocking arrangements for abhorrent violent material is to prevent terrorist threats such as those of the Christchurch terrorist attacks.[2] This completely ignores the motives behind these attacks, and how they were orchestrated.

Furthermore, publicly posting such material has often lead to arrests due to the tips of users.[3] Such tips have even led to the occasional foiling of a terror plot.[4]

# In conclusion

Many service providers already have content moderation policies which bans or restricts objectionable content, which is enforced heavily. The Australian Government must maintain a good working relationship with service providers to combat cyber-crime for a cyber-safe Australia.

Any legislation which could potentially impact the relationship the Australian government has with the private sector, or members of the public, has potential economic and national security impacts, which must be assessed.

Furthermore, a suitable balance must be struck; the legislation as proposed currently over-steps this balance in the wrong direction.

# References


1. Fact Sheet—Online Safety Bill
   https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act
2. Consultation on a Bill for the New Online Safety Act
   https://www.communications.gov.au/have-your-say/consultation-bill-new-online-safety-act
3. Tip From 4chan Leads To Arrest Of Site Visitor On Child Porn Charges
   http://www.thesmokinggun.com/buster/4chan-reports-child-pornographer-769123
4. Shooting threat at 4chan leads to arrest, closure of over 20 Dutch schools
   https://www.theverge.com/2013/4/22/4252042/shooting-threat-4chan-leads-to-arrest-dutch-school-closings