Inquiry into cyberbullying: Questions on Notice

1. Transparency and use of Statistics

"Do you see a role for transparency (by Social Media Services) in those statistics (statistics around cyberbullying)? Would that be something you'd like to see changed? Would that help your office better understand who you're dealing with? Would that data, if it were made available, be useful for you?"

We work closely with social media services who have complied with 100% of our requests for removal of cyberbullying material. The Office proactively engages with industry and considers that the policies and practices of the large social media services to address cyberbullying are working.

To date, social media platforms have not been required to provide transparency reports on the numbers of cyberbullying reports they receive, and number of accounts frozen and/or deleted as a result of serious breaches.

Data about cyberbullying and other abuses collected by the social media services would be useful to have. For example, the information might be used to target resources, raise awareness, and provide education on specific issues.

However, it is unclear how much weight we could place on this type of information. There are two reasons for this. The first is that user-flagging of objectionable material on a service will always rely on the specific rules, guidelines or standards applicable to that service, rather than the statutory thresholds employed by the eSafety Commissioner. The second is that the data, being user-generated and unverified, may not reliably reflect the *actual* incidence of cyberbullying on a platform.

2. Demographic data of cyberbullying reports

"I wonder whether you might… be able to provide any information you've collected regarding those that have reached out to you to access these services—demographic data and basically anything you collect when you interact with them around gender, socioeconomic status or even location…"

Cyberbullying manifests itself in many forms. We know that approximately 1 in 5 Australian children are cyberbullied. Girls are cyberbullied more frequently than boys, although an increasing number of boys were targets last year. Most common forms of cyberbullying include social exclusion, name-calling, and the spreading of lies and malicious rumours.

Our experience shows that children and teens are predominantly bullied online by those in their own peer group. In many instances, cyberbullying is an extension of bullying or conflict occurring within the school. In reports to the Commissioner about cyberbullying, victims often note that the harassment they experience online broadly mirrors their experience at school. Further, the perpetrators are in many instances one and the same.

Key data:

- For the period **1 October 2017 to 31 January 2018**, cyberbullying complaints to the Office increased by 30%, compared to the same period last year.
- The majority of complaints relate to tier 2 scheme members, with complaints concerning Instagram (43%) and Facebook (27%) the most prevalent during this period.
- Tier 1 social media services accounted for 15% of complaints during this period.
- 60% of complaints were from females.
- The average age of a complainant was 14 years.
- Almost 20% of complaints involve victims (and perpetrators) who are aged under 13 years of age.
- Almost 90% of complaints are lodged by the child or a parent – 50% children and young people; 40% parents. The remainder are complaints lodged by an authorised adult (such as a teacher) on a child's behalf.
- Across States and territories, the following breakdown of complaints was received:
    - NSW 28%
    - QLD 23%
    - VIC 20%
    - ACT 7%
    - SA 7%
    - TAS 5%.

Our research shows that young people are less likely to use formal channels in order to seek redress, guidance or support. Only 50% of young people turn to their family and informal support networks for assistance. Around 13% involve their school and only 12% reported what happened to the social media websites. Fewer still – 2% – referred the matter to the police.

3. Average time line from contact to content being taken down

"Do you have an average time line from when somebody reaches out to you with an issue to that issue being taken down?"

From 1 October 2017 to 31 January 2018:

- The average length of time between the Office requesting removal of content from a social media service, to the Office being informed that the material has been removed, was 39 hours.[1]
- The fastest time for content removal by a social media service following a request by the Office was 26 minutes.

In order to determine whether content has been taken down, the Office relies on two methods: direct notification by the social media service, and manual checks by Office investigators.

[1] It is important to note that this is reflects the time between a request by the Office and *notification* by the social media service. In the majority of cases, material will have been removed well before notification.

4. Average time spent per case.

"Would you be able to let us know the average time you spend per case that you deal with? We've got 30 seconds for social media companies. I'd really love to know how much time each of your people spends."

The complaints received by the Office are diverse in nature and many involve unique circumstances. From 1 October 2017 to 31 January 2018:

- We responded to 97% of all complaints about cyberbullying within three hours.
- We resolved complaints, on average, in 150 minutes.[2]

5. Information requested relation to s.230 of the *Communications Decency Act* 1996 (USA) as of 2 March, 2018

"Do you have any detail about that (Communications Decency Act), even if you can point us in the direction of some journal articles or where you get your information on that?"

Section 230 of the *Communications Decency Act* shields internet services and technology companies from liability based on a third party's content in subsection (c)(1): "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

There is widespread belief that s.230 has been one of the most important provisions protecting free speech online, allowing internet service providers freedom to publish others' content without reviewing it for criminality or other legal issues. Equally, many believe that these liability protections are too broad. It is argued that they are being used as a defensive shield against a wide range of online ills, including sex trafficking, and consequently that a limit to the provision's scope is required.

Some Members of Congress have introduced bills to abrogate s.230's shields in certain circumstances (in particular, the *Stop Enabling Sex traffickers Act* of 2017 (SESTA), and the *Allow States and Victims to Fight Online Sex Trafficking Act* of 2017 (FOSTAhttps://www.congress.gov/bill/115th-congress/house-bill/1865?r=1)). The House of Representatives passed the FOSTA bill on 27th February, 2018, and the bill will now be passed to the Senate.

There has been a strong backlash against such amendments, due to the unintended consequences that abrogating the shield could have, for example preventing sex workers from sharing helpful information online. It has also been repeatedly highlighted that s.230 does not immunize against unlawful conduct, and that uniformity of the application of this federal policy to all crimes is necessary (the above bills focus on sex trafficking).

---

[2] This involves the first substantial action taken to resolve a complaint (for example, making a referral about content to a social media service for takedown).

A Concurrent Resolution has been proposed, to restate the clear intent of s.230, and to re-emphasise the denial of protection to internet *platforms* that are partly complicit in the creation or development of illegal content.

Also of note are developments in the North American Free Trade Agreement (NAFTA). A group of academics and organisations have sought to incorporate intermediary immunity into NAFTA.

Globally, pressure has been placed on ensuring that internet service providers are held to account for the content on their platforms. Advancements in technology have meant that illegal content can be identified and removed expediently and effectively – and as such, it is arguable that an onus should be placed on providers to embed these tools into their products (safety-by-design). Once a provider is made aware of such content, it should be their duty to remove it, or to take reasonable and proportionate steps to remove such content. When this has not been carried out, they should be held liable for that content.

Concerns relating to s.230 are indicative of a shift, both politically and socially, about the roles and responsibilities of internet service providers. The debates that are centred on the *Communications Decency Act* are reflective of a realisation, given the ubiquitous nature of the online world, that existing structures and policies relating to how the internet is governed, and how it should be regulated, are outdated and in need of reform.

6. Information requested re: key EU and Global activity, as of 2 March, 2018

"You mentioned the EU, and we have had some discussion about that here. So there is a change in direction in the EU. If you have any information on that, that would also be helpful."

Germany has passed a new law requiring internet platforms with over two million users to proactively report and delete unlawful content. The Netzwerkdurchsetzungsgesetz (NetzDG) law, or *Enforcement on Social Networks Act*, was passed at the end of June 2017 and came into force in early October.

On 1 March 2018 the EU Commission recommended a set of operational measures to be taken by companies and member States to step up on tackling illegal content online, before it determines whether legislation is required. Member States and companies are required to submit relevant information on terrorist content within three months, and other illegal content within six months.

On 25 May 2018, a European privacy law, the *General Data Protection Regulation* (GDPR), is due to take effect. The law aims to set a new global bar for privacy rights, security, and compliance. Under the GDPR, social media platforms will have to abide by strong compliance obligations in relation to personal data. The impact of the GDPR will also have a global impact. The GDPR has left open many legal interpretations on key issues relating to children; particularly in relation to age verification, data profiling and consent-based data processing.

The EU's *Audiovisual Media Services Directive* (AVMSD) is currently under review, with new legislative proposals being considered – including the prohibition of hate speech and the protection of minors. In addition, video-sharing platforms will now be included in the scope of the AVMSD to address these factors, which are fully in line with the ecommerce Directive.

The UK are currently developing an Internet Safety Strategy. As part of this process, the UK Government is seeking to:

- develop a Code of Practice which seeks to develop new standards for online platforms, spearheaded by the Information Commissioners Office
- introducing an annual internet safety transparency report – providing UK data on offensive online content and what action is taken to remove it
- reviewing current legislation on offensive online communications to ensure that laws are up to date with technology

A number of inquiries have taken place globally incorporating debates on self-regulation, accountability and transparency of social media platforms:

- Australian Competition and Consumer Commission (ACCC) inquiry into the impact of digital search engines, social media platforms and other digital content aggregation platforms on the state of competition in media and advertising services markets.
- UK Parliament's Home Affairs Committee Inquiry into "Hate crime and its violent consequences", the House of Lords Select Committee "Growing up with the Internet", and the Committee on Standards in Public Life "Intimidation in Public Life".
- In France, President Emmanuel Macron has recently announced plans to legislate to tighten the rules on what content social media companies can permit to be posted on their sites during elections.
- A High-Level Expert Group has been set up to contribute to the development of an EU-level strategy on how to tackle the spreading of fake news and disinformation.