

## **Re: Improving the Office's access to social media service account data**

US-hosted social media services (SMS) will generally accept requests from foreign law enforcement to preserve records connected with an official investigation. For example, Twitter will hold relevant account data for 90 days pending service of a valid legal process. However, all require formal court or treaty documents to be served before they will release account data to a foreign police agency.

Facebook, SnapChat and Twitter all refer to their obligations under Title 18 of the United States Code, section 2703, which requires that subscriber information will be provided to a government entity on presentation of a warrant, subpoena or other court process, or via the Mutual Legal Assistance Treaty (MLAT).

To give effect to its regulatory powers – specifically where End-User Notices are concerned – the eSafety Office could apply to the Federal Court for a subpoena supporting access to SMS account data. However, without the ability for eSafety to first preserve the data, any value in a court order is questionable. This constrains the application of the cyberbullying End-User Notice scheme where eSafety is unable to establish a perpetrator's identity from public records.

To help facilitate our access to SMS account data, there may be merit in considering a written arrangement whereby we seek assistance from the AFP to make a preservation request from a social media service on our behalf. Once in place, eSafety would then be responsible for making all necessary applications to the Federal Court for the relevant order. Such assistance would be sought only in the most serious of matters, those that fall just short of warranting referral by eSafety to state or territory police.

An arrangement of this kind would acknowledge the role of the AFP as eSafety's Commonwealth law enforcement partner. It might be further reinforced by an agreement dealing with how limited Australian person-of-interest intelligence pertinent to a cyberbullying investigation might be provided to eSafety by the AFP in certain circumstances.

## **Review the Enhancing Online Safety Act 2015 to strengthen the cyberbullying scheme**

To remain effective, the Office must be able to act on abuse material across the spectrum of digital devices, services and platforms that enable cyber abuse and cyberbullying to occur due to their interactivity capabilities.

The Act currently allows the Office to intervene in a wide variety of instances involving cyberbullying. The definition of a social media service is set out in s. 9 of the Act. However, there is uncertainty over whether certain online service providers that permit the sending of cyberbullying material (anonymous apps such as Sarahah, various gaming services), are able to be considered a 'social media service' within that definition.

If the service is not a 'social media service' within the Act then the Office is left with little recourse to assist affected persons. This aspect will become increasingly more problematic as these types of platforms become more popular. It would be useful to bring these platforms under the tier scheme.

**Louise Pratt MP**  
**Chair**  
**Senate Legal and Constitutional Affairs Committee**  
**By email:**

Dear Louise:

While I agree that the most egregious forms of cyberbullying may warrant criminal intervention, I am concerned that a punitive emphasis will produce a range of undesirable outcomes. For example, subjecting children to a greater range of criminal penalties will almost certainly lead to higher rates of formal supervision by, and even remand within, juvenile justice systems. As well, new criminal offences may place strain on already stretched police resources, nationally.

Based on what we have seen effectively work, my preference is to promote early intervention and prevention approaches over punishment and deterrence, and I have outlined a number of potential alternatives below. Ideally, these options would work in concert as complementary elements of a single and coherent national strategy.

*The need for a greater awareness of the Office, and our role*

The Office is not always made aware of a problem with cyberbullying material in time to act. Although we are experiencing a steady increase in the number of cyberbullying complaints, there is a critical need to do more to raise awareness of the Office. This is especially true where rural and regional Australia is concerned. With adequate resourcing, the Office could launch a national awareness-raising campaign encouraging young people across Australia to reach out to and report harmful online material to us.

*Research into best practice initiatives*

ReachOut has published research showing that about half of all young people who are targeted by cyberbullying seek help from parents and other trusted adults. Further research into best practice approaches to targeting resources and information to vulnerable young people would be valuable.

*A comprehensive peer support program*

Because we understand the crucial role played by peers in support of cyberbullying victims, the Office is currently scoping a 'digital leaders' program as an unfunded pilot. An expanded program could equip young people to work as leaders in confronting online issues within their school or peer group. This could provide every school with a trained youth-led team, supported by an accredited teacher professional program that students can go to for help if they are being cyberbullied.

*Review the Enhancing Online Safety Act 2015 to strengthen the cyberbullying scheme*

There are several areas of the cyberbullying scheme which might benefit from review. One concerns the definitions of ‘social media service’ and ‘relevant electronic service’. Neither provide sufficient clarity, and do not necessarily work well to capture all channels along which cyberbullying of children occurs – for example, gaming platforms such as Playstation and Xbox Live. I am also concerned that the definition does not encompass anonymous social interaction apps– such as Sarahah – that are often used for bullying.

In addition, the Act’s basic online safety requirements should be strengthened by including the need for social media services to demonstrate they have in place robust user settings and terms of use, clear and unequivocal community standards, and a proactive approach to dealing with cyberbullying on the platform.

*Widening the scope of the Enhancing Online Safety Act 2015 to apply to vulnerable adults*

Since the remit of the Office was expanded in June 2017 to cover *all* Australians, we have been contending with a growing number of complaints from adults who are experiencing cyber abuse. There is possible merit in extending the operation of the cyberbullying scheme to cover vulnerable adults.

Clearly the question of how the definition of who is a vulnerable adult is relevant to this question. The term might include those with an intellectual disability, developmental disorder or mental illness; Aboriginal or Torres Strait Islander people or those from a non-English speaking background; and women experiencing domestic violence. Any extension of the scheme should come with additional resourcing.

Yours faithfully,

Julie Inman Grant  
**eSafety Commissioner.**