Australian Government | eSafetyCommissioner

16 February 2023

Committee Secretary
Select Committee on Foreign Interference through Social Media
Via: foreigninterference47parl.sen@aph.gov.au

Inquiry into Foreign Interference through Social Media

The eSafety Commissioner (eSafety) is Australia's independent regulator for online safety. Our purpose is to help safeguard Australians at risk from online harms and to promote safer, more positive online experiences.

eSafety's legislative functions are provided by the *Online Safety Act 2021* (OSA). This includes coordinating online safety activities across the Australian Government, supporting and conducting educational and community awareness programs, and administering four regulatory complaints and investigations schemes, including cyberbullying of children, cyber abuse of adults, the non-consensual sharing of intimate images, and illegal or restricted online content. We also have powers to regulate social media platforms' broader systems and processes.

While foreign interference is not a matter that falls directly within eSafety's remit, we recognise that this activity has the potential to intersect with eSafety's responsibilities in at least two areas. First, eSafety has a role in promoting industry's adoption of Safety by Design and compliance with the government's Basic Online Safety Expectations (BOSE) to prevent and mitigate harms to users resulting from existing and emerging online threats and harms. In addition, matters which are reported to eSafety for investigation under our four regulatory schemes may, in rare cases, involve an element of foreign interference. We work collaboratively with responsible Departments and agencies to provide a holistic response to these issues.

Recommender systems and algorithms

eSafety closely monitors technology trends which may present risks to Australians' online safety or challenges to our ability to regulate online harms.

As part of this work, eSafety recently published a position statement on recommender systems and algorithms, which was informed by extensive consultation with academics and other subject matter experts.

Our position statement found that while recommender systems and algorithms have positive uses, they can also present an array of risks to users. One of these risks is the potential to amplify harmful and extreme content, particularly when used by platforms whose content feeds are driven by user engagement.

The amplification of content that promotes division, false narratives, and undermines democratic values may have adverse effects, such as normalising prejudice and hate and distrust in public institutions. It may also contribute to radicalisation towards terrorism, violent extremism, and provide users with avenues to find associated groups.

While countering violent extremism and disinformation are issues that primarily sit with other Commonwealth entities, including the Department of Home Affairs and the Australian Communications and Media Authority (ACMA), eSafety's regulatory complaints and investigations schemes can assist in remediating harm by facilitating removal of harmful content which meets relevant thresholds, and by providing support and advice to Australians who may be affected these harms about how to stay safe online.

We are also undertaking a number of regulatory approaches to increase platforms' transparency and accountability on their use of algorithms, including exercising new powers under the OSA.

Anonymity and identity shielding

Anonymous communication is seen by many as a cornerstone of promoting freedom of speech, expression and privacy on the internet, however it can also pose a risk to Australia's democracy and values.

When a user is able to hide or disguise their identifying information online, it can make it extremely difficult for regulators and law enforcement to identify them and hold them responsible for what they say and do online. These actions can be used to exploit sentiment, trust and fuel dis/misinformation and propaganda initiatives.

Our investigations have shown this as a common tactic used by those who seek to harm or cause abuse online. As highlighted in the Department of Home Affairs' submission, it has also been deployed by state-based actors to exert power and influence operations during times of war and conflict.

Software, browsers and anonymous platforms may be used for identity shielding. Examples include virtual private networks (VPNs) that mask the user's location and device details (IP address), and anonymising processes that conceal the link between a message and the sender.

eSafety takes a number of approaches to prevent and deal with potential harms stemming for anonymous and fake accounts. This includes working with individuals and industry to raise awareness about potential safety risks and ways to protect themselves, supporting victims who have reported abuse from anonymous or fake accounts, and encouraging proactive change from industry through the uptake of our Safety by Design initiative. Under the BOSE, we can also require service providers to respond to questions seeking transparency on the reasonable steps they are taking to prevent harmful use of anonymous services.

Further detail on current industry practices and potential safety risks can be found via our position statement on anonymity and identity shielding.

Online harms affecting vulnerable communities

eSafety aims to provide support to a range of communities and groups, particularly to those most at risk of online harm. Our regulatory schemes can assist individuals who may be susceptible to foreign interference, such as diaspora groups, those with low digital literacy, and minority groups who may be the target of cyber abuse and illegal activity. These schemes intersect on a range of issues to provide multiple avenues of support.

In addition to targeted misogynistic abuse and gendered disinformation, women in the public eye who challenge autocratic leaders, traditional male power structures or human rights and gender issues tend to attract more organic and coordinated vitriol online.

eSafety conducts research and provides support through our educational and training programs. For example, as part our Women in the Spotlight (WITS) program, eSafety provides strategies, advice and social media self-defence training, which seeks to elevate and protect women's voices online and build their digital resilience.

Our online safety resources are also available in a variety of community languages to ensure our work remains clear and accessible to a range of communities.

eSafety appreciates the opportunity to contribute to this inquiry and would welcome our inclusion in any further engagements on relevant matters.