Australian Government
Department of Home Affairs

Department of Home Affairs submission to the Inquiry into Social Media and Online Safety

Select Committee on Social Media and Online Safety

12 January 2022

Table of Contents

Overview

1. The Department of Home Affairs (the Department) welcomes the opportunity to provide a submission to the Select Committee on Social Media and Online Safety.

2. The digital environment has transformed our economy and society, delivering significant benefits for Australians. However, the breathtaking leaps forward in connectivity have been accompanied by equally stunning abuses of communication and technological tools. These benefits and challenges need to be effectively balanced. Australia's regulatory architecture should support this objective, with innovative reforms pursued where needed to effectively address the increasing influence of technology on social, economic, political and security domains.

The risk to Australians from online harms is at unprecedented levels – and getting worse

3. Government and industry have been naïve in thinking the online domain would be free from the evils that have afflicted the physical world. We now better understand the role digital platforms can, and often do, play in the deteriorating safety and well-being of our community. This includes harms at an individual level by enabling the global scale proliferation of child sexual abuse material (CSAM); at a societal level with the active promotion of misinformation and disinformation leading to declining trust and civility; the fragmentation of our national discourse through echo-chambers and filter bubbles; and the spread of violent extremism material undermining our social cohesion.

4. Compounding the problem is the adoption by digital platforms of technological enablers and amplifiers. The use of anonymising and oblivious technologies such as end-to-end encryption and persuasive algorithms are making online harms more prevalent and harder to identify. As outlined below, the use of algorithmic promotion is of particular concern given the potential harm it can cause to our society, including children, all in the name of generating product growth and revenue for digital platforms. The Department considers enabling and amplifying technologies as some of the most pressing issues in the online harms space in need of addressing. This is because they are systemic in nature. They cut across almost all types of online harms exacerbating already challenging problems.

The response from digital platforms has been slow, incremental and minimal

5. Government has sought to regularly engage with industry to develop creative and technology-driven solutions that would enable a better balance between the tremendous opportunities enabled by digital platforms and the legitimate safety needs of the community. In order to achieve this balance, Government has long encouraged industry to adopt a safety-by-design approach that prioritises the safety of users in the development of their products rather than 'bolting on' safety features once those products have been exploited.

6. Digital platforms continue to be manipulated by malicious actors, and those seeking to do harm are able to exploit their technologies faster than industry can develop new safety features. The world-leading innovation demonstrated by many digital platforms in developing their products and services has not been evident when it comes to addressing user safety. While not alone, amongst the "big tech" companies, Meta is frequently the most reluctant to work with Government to promote a safe online environment, adopt a safety-by-design approach and take adequate proactive measures to prevent online harms.

More is needed to turn the tide

7. Australia has been world leading in its proactive regulatory approach to mitigating the risks of online harms. Pioneering actions to address competition issues (through the News Media and Digital Platforms Mandatory Bargaining Code), online safety (through the *Online Safety Act 2021*, *Online Privacy Act 2021* and the Social Media (Anti-Trolling) Bill) and security (thorough the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018,* among others), have demonstrated that even a relatively small market like Australia can shape the practices of global platforms.

   While these initiatives have been effective, they have not yet brought about the comprehensive cultural change required for digital platforms to make user-safety a first order priority.

8. Governments are accountable to their citizens for making the laws that govern our society – whether online or offline. Digital platforms are accountable only to their shareholders and their consumers. It is therefore appropriate that the Parliament, as the representatives of the citizenry, continue to determine the rules by which we live. It is that rule of law, and not the terms of service set by multinational corporations, that should set the standard and ensure the online safety of all Australian users.

Enabling and amplifying technologies

9. There are increasing concerns in both Australia and other nations, about the influence, reach and harm caused by technological enablers and amplifiers across digital platforms, including persuasive technologies like algorithms, and anonymising and oblivious technologies like end-to-end encryption. These technologies intersect with, and enable, all types of online harms.

Algorithmic persuasion

10. Digital industry's financial interest in attracting and retaining users has led them to implement **algorithmic promotion** of material on their platforms. Algorithms are used to selectively predict the information that a user is more likely to engage with based on information about the user, such as location, past click-behaviour and search history. Digital platforms currently employ algorithms to target users with content that appeals to their interests (filter bubbles).

11. As a result, users can become separated from information that is contrary to their viewpoints, effectively isolating them in their own cultural or ideological bubbles. These technologies can create digital echo chambers where users are fed the same information, and encouraged to interact or join groups of people who share the same viewpoints, while differing opinions or information is not brought to their attention. Filter bubbles and echo chambers can reinforce an existing opinion within a group and move the entire group toward more extreme positions. This can fuel racism, violence, and extreme political and/or ideological views and play a key role in radicalising individuals by continuously feeding extremist narratives. It is becoming clear through research by experts like Hany Farid, and the release of papers by Frances Haugen, that algorithmic promotion is almost singularly responsible for the toxic disinformation environment online.

12. Testimony provided to the US Senate from former Facebook employee, Frances Haugen, has also confirmed that digital platforms are, sometimes knowingly, promoting harmful and divisive content which tends to generate user interest and therefore revenue, as they pursue policies that prioritise company growth over public safety. In some instances, Facebook was aware that their algorithms aggravated polarisation of dangerous views, increasing the effect of echo chambers to manipulate user behaviour and encourage and reinforce extreme ideologies.

13. The algorithmic promotion of such content leads to a toxic information environment and creates division damaging our social cohesion. Such revelations call into question long held views that digital platforms were passive channels. The fact that platforms are actively selecting and promoting content using an algorithm raises questions about whether they are acting as publishers and should be regulated as such.

14. In addition to algorithmic promotion, digital platforms have also adopted **persuasive design** techniques. That is, design approaches conceived by human developers to maximise a user's engagement, usually tapping into social rewards and psychological behaviour, such as social reciprocity on social media platforms; pull-to-refresh content; or "streak rewards" in games or social messaging platforms. These designs reinforce and reward behaviours, such as people "liking" or "sharing" content. By expanding this and "pushing" content at users via notifications and reminders, people are being conditioned to constantly engage with and even rely on these platforms and services, becoming digitally dependant.

15. Platforms that use persuasive technologies to increase and retain our attention have been shown to have negative impacts on user health and wellbeing. Social media in particular triggers feelings of sadness, isolation, and dissatisfaction with our lives.[1] The ABC's "Australia Talks" survey found that 22% of Australians felt worse about themselves when viewing other people's social media posts. Young people felt this the most deeply, with 45% of 18-24 year olds and 43% of 25-29 year olds agreeing.[2]

16. It is important to note that AI and algorithms can also serve a benefit in reducing online harms. Both are already utilised by some social media platforms to block child grooming conversations. However, in a survey conducted by the WeProtect Global Alliance in partnership with the Technology Coalition, only 37% of companies who responded actively implemented such technology to counter threats of child grooming.[3] This is concerning, as recent research has demonstrated that Facebook's Friend Finder function has been exploited by child sexual abuse live streaming facilitators to connect them with offenders.[4]

Potential policy responses

17. The Department has significant concerns about the far-reaching consequences that persuasive design and algorithms have for both individual users and social cohesion more broadly. The Department is currently exploring potential policy and regulatory responses.

18. This is not a problem unique to Australia, and a number of solutions are being considered in other jurisdictions including:

    - improving the transparency and oversight of the use of persuasive design and algorithms;
    - compelling public disclosure of internal company data and research to allow independent analysis and accountability; and
    - establishing regulatory frameworks that prioritise child and community safety over business growth.

19. More targeted proposals, such as the US' proposed *Filter Bubble Transparency Act*, which is intended to provide users with more options including to 'opt out' of seeing optimised content, also offer potential ways forward.

Anonymising and oblivious technologies (including end-to-end encryption)

20. Organised and dangerous criminals are increasingly utilising anonymising and oblivious technologies, such as end-to-end encryption, peer-to-peer networks, decentralised networks, cryptocurrencies and virtual private networks to conceal evidence of crimes – including communication and financial transactions – to avoid traditional law enforcement identification and investigation techniques. The increasing normalisation of these technologies on digital platforms, including social media, is bringing Dark Web functionality to the mainstream.

21. Despite the well-founded concerns of Governments, law enforcement agencies and non-government organisations in relation to these technologies, large digital platforms continue to use prolific encryption. While strong encryption plays an important role in protecting user privacy and data, the use of this technology in some settings, particularly on platforms used by children, brings with it important public safety risks. The application of end-to-end encryption across social media messaging services – such as expansion beyond the current opt-in services proposed by Meta (including on platforms such as Messenger and Instagram Direct) – will provide predators with the ability to evade detection as they connect with multiple vulnerable children anywhere in the world and develop exploitative grooming relationships. The nature of end-to-end encryption means that not even Meta, as the hosting company,

[1] Schaurgin O'Keeffe G, Clarke-Pearson K, 'The impact of social media on children, adolescence, and families', *Pediatrics,* vol. 127, issue 4, 2011.
[2] A 2021 survey of over 60,000 Australians developed by the ABC, in collaboration with social and data scientists from Vox Pop Labs. The University of Melbourne was the Australian academic partner on the project, with additional input from an advisory panel of academics from other Australian universities.
[3] Global Threat Assessment 2021, WeProtect Global Alliance (https://www.weprotect.org/).
[4] Napier S, Teunissen C & Boxall H, 'How do child sexual abuse live streaming offenders access victims?', *Trends & Issues in Crime and Criminal Justice* no. 644, 2021.

would be able to retrieve or view these messages in order to detect child abuse, even under a lawfully issued warrant. The anonymity afforded by end-to-end encryption not only enables predators to groom victims on a social media platform, it also allows these criminal to safely connect and share tactics on how to perpetrate child sexual abuse, share explicit images, arrange live streaming of child sexual abuse through facilitators in vulnerable countries and avoid law enforcement.

22. The Department has ongoing concerns that digital platforms are prioritising privacy to the detriment of public safety. The Department's engagements with Meta and other companies with 'privacy first' polices reveal a degree of seeming indifference to public safety imperatives, including in relation to children. For example, end-to-end encryption provides limited advantages over and above network level encryption. In the case of Facebook Messenger for example, end-to-end encryption will only apply to the content of messages, which has less commercial value to the company. The Department understands that personal data, such as metadata and site and cookie tracking, could still be exploited by Meta for commercial purposes, in line with their business model.

Policy responses

23. Debate on end-to-end encryption has become increasingly polarised, and some privacy advocates argue that, in the application of end-to-end encryption, it is all or nothing. The Department reject this.

24. Digital industry have demonstrated that tools can be developed to scan for child sexual abuse material in a fully end-to-end encrypted environment. For example, in August 2021 Apple announced the rollout of a new feature called 'NeuralHash', which allows on-device scanning of images to detect child sexual abuse material on iOS devices. The new feature will reportedly detect a hash match against a database of known child abuse imagery before an image is uploaded to iCloud Photos, within an end-to-end encrypted ecosystem. Child sexual abuse material that is detected will then be referred to the US-based National Center for Missing and Exploited Children (NCMEC) for triage and investigation. Unfortunately the announcement from Apple was met with significant backlash from privacy advocates, and it is now unclear if Apple will implement this technology as previously intended.

25. The Department continues to encourage industry to identify technical solutions that better balance privacy and safety. Digital platforms should also adopt safety-by-design principles across their technologies and services, in accordance with the message in the *International Statement: End-to-End Encryption and Public Safety*.

26. The Government, supported by the Home Affairs Portfolio, has introduced a number of recent legislative reform packages to address some of the challenges that new technologies, such as anonymising technologies like encryption pose to law enforcement, including the:

    - *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*, which introduced an industry assistance framework to allow law enforcement and security agencies to seek or require assistance from industry to access important data to support investigations, and a computer access warrant framework to improve the ability for law enforcement agencies to access content at an unencrypted point.

    - *Telecommunications Legislation Amendment (International Production Orders) Act 2021*, which reshapes Australia's international crime cooperation efforts by addressing the challenges associated with obtaining electronic data held offshore, for example, social media companies based in the US. This will significantly enhance the ability of our law enforcement and national security agencies to investigate serious crimes, particularly those that are technology-dependent like ransomware and other cybercrime offences, child sexual exploitation and abuse, and serious and organised crime.

    - *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, which introduced three new powers to enable the AFP and ACIC to collect intelligence to expose criminal networks operating online, disrupt their activity and gather evidence to support prosecutions.

27. In response to the recommendations of the Comprehensive Review of the legal framework of the National Intelligence Community, the Government is also progressing holistic reforms to Australia's electronic surveillance laws. Our existing laws have struggled to keep pace with technological change and digital communications, such as the rapid uptake of social media and other digital platforms. The reforms will provide clear, transparent and usable powers, with appropriate safeguards, to support agencies to keep our community safe online as technology continues to evolve rapidly. The Department has established an interagency taskforce to work across government and other key stakeholders, including communications technology providers and the public, to deliver this reform by 2023.

Online harms on digital platforms

28. While addressing technological enablers and amplifiers would have broad ranging online safety benefits, the Department is also focused on understanding and addressing specific online harms. In line with the Committee's terms of reference, the Department has focused this part of the submission on online safety issues for children. However, the Department notes that the spectrum of online harms is far broader than the online safety of children – including misinformation and disinformation, foreign interference, cybercrime, and violent extremism. A brief summary of these issues is set out at the bottom of this section. The Department would welcome the opportunity to explore these issues further with the Committee.

Child sexual abuse material, including live-streaming

29. Information and communications technologies have provided a vehicle for the proliferation of child sexual abuse at a global scale, and created an online market for the exchange of child abuse material. The rapid adoption and evolution of communication technologies have provided offenders with easier access to CSAM; enabled the online coercion, manipulation and grooming of children; and increased networking capabilities for offenders to share abhorrent CSAM and tradecraft. The scale and complexity of this increasingly borderless crime is compounded by the ubiquity of technology in the context of the COVID-19 pandemic. Isolation requirements have increased the time that children and offenders are spending at home and online. Offenders are actively seeking to exploit these conditions to offend, increasing the threat of online harm to children.

30. Social media has provided a vehicle for the proliferation of CSAM over the open web. Image hosting websites, including social media platforms, remain the most common site type used to distribute child sexual abuse imagery. The volume of CSAM online continues to grow exponentially. In 2020, NCMEC received 21.7 million reports of child sexual abuse comprising 65.4 million images, videos and other files. Methods of producing and sharing CSAM are constantly changing, assisted by increased widespread connectivity and technological development. Additionally, the scale and severity of online offending has escalated over time, with material now depicting increasingly younger children and higher degrees of violence.

31. The Australian Centre to Counter Child Exploitation (ACCCE) identifies 'capping' as an increasingly problematic offending methodology. 'Capping' involves offenders targeting children on a variety of online platforms. After developing a level of trust with a child, they are coerced to perform sexual acts, which the offender captures on camera. Material is then frequently shared with offending networks. 'Capping' has generated 60-70 per cent of referrals to the ACCCE's Victim Identification Unit. In their Global Threat Assessment 2021, the WeProtect Global Alliance highlighted that the increased prevalence of 'capping' illustrates the potential 'gamification' of abuse: dark web forums host competitions and 'capping battles' where offenders compete by posting the abusive imagery they have produced.

32. Other forms of online child abuse offending are increasing. NCMEC statistics for 2020 revealed a 97.5 per cent increase in 'online enticement' of children, including grooming for the purposes of sexual abuse, linked to the circumstances arising from the COVID-19 pandemic. Online grooming can also lead to contact sexual abuse, as a result of coercing a child to meet with the perpetrator. Similarly, in 2021, the ACCCE identified an increase in Member of the Public (MoP) reports of children self-producing CSAM for financial incentives, with children as young as 10 years old being targeted with incentives such as in-game currency on popular online games. Children coerced to create self-generated sexual imagery may not view themselves as victims and can perceive their actions as voluntary.

33. Police face a range of challenges combatting online child sexual abuse. For example, it is common for offenders to seek to migrate conversation from public to private messaging platforms where communication is protected by end-to-end encryption, or to newer platforms that lack robust user-safety mechanisms. This behaviour, referred to as 'off-platforming', is a tactic that poses significant challenges for law enforcement to detect offenders. Live-streamed child abuse, while comprehensively criminalised, is a rising area of offending. Live-streamed abuse is becoming increasingly prevalent, enabled by connectivity and the availability of inexpensive streaming devices and the availability of video call functionality on social media. While the real-time abuse primarily occurs in South-East Asian countries, and in particular the Philippines, content consumers are predominantly located in Europe, North America and Australia. Offenders often engage with this material in exchange for money and specify the type of abuse they wish to see. This differs from other CSAM as the offenders are often directing and requesting specific abusive and exploitative acts to occur against the children in real-time that can be sadistic in nature. Recent evidence shows that live-streamed abuse is occurring via mainstream platforms on the open web.

Industry measures

34. The design of platforms and services and the efforts of industry, in cooperation with government policy-makers and law enforcement, are critical to addressing these challenges and ensuring offenders cannot evade detection and continue inflicting immense harms on children.

35. The Technology Coalition is a global alliance of 24 leading technology firms (50 per cent of whom offer social media services) that have come together to build tools and advance programs that protect children from online sexual exploitation and abuse. The Department works closely with the Technology Coalition to advocate for stronger voluntary standards and encourage collaboration with policy makers and civil society.

36. The WeProtect Global Alliance, in partnership with the Technology Coalition, surveyed Technology Coalition members for their Global Threat Assessment 2021. The survey revealed that, while most companies use tools to detect child sexual abuse material (87% use image 'hash-matching'), only 37 per cent currently use tools to detect the online grooming of children. End-to-end encryption considerably reduces the efficacy of hash-matching detection tools such as PhotoDNA. With the increasing prevalence of CSAM in video format, greater investment from industry in video scanning or detection technologies is required.

Technology Coalition Annual Report 2021

Technologies such as PhotoDNA enable tech companies and organizations like NCMEC to assign unique "hash-based" alphanumeric identifiers to images of known CSAM. These "hashes" of known CSAM images are compiled and used by industry to detect further attempts to upload known CSAM to their platforms and to report, remove, or block upload of those images. The hash-based technology for detecting still images is mature and operates on a common hash format used across industry. Hash-based video detection is less developed, and there is not yet an industry standard hash format.

All Technology Coalition Members currently deploy or are in the process of implementing hash-based technology that detects known CSAM images. PhotoDNA remains the most popular image hash-based detection tool for members, used by 75 per cent of companies, with MD5 second most prevalent (38 per cent). 54% of Members currently deploy video hash-based detection technology, with CSAI Match (33 per cent), PhotoDNA for Video (25 per cent) and MD5 (25 per cent) being the most commonly used video hash-based detection tools. 38% of Technology Coalition member companies contribute hashes or keywords to NCMEC's industry hash repository and eight per cent contribute to the Canadian Centre for Child Protection's Project Arachnid.

Transparency and accountability required of digital platforms

37. Voluntary cooperation, transparency, legislation and regulation must be complementary to tackle this fast evolving space. On 5 March 2020, Ministers from Australia, UK, Canada, US and New Zealand launched the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, which provide a high-level, best practice framework to guide online platforms and service providers to address the risk of online child sexual abuse.

38. The Voluntary Principles were developed in partnership with digital industry (namely Facebook, Google, Microsoft, Roblox, Snap, TikTok and Twitter), non-government organisations and academia. The Voluntary Principles cover issues ranging from online grooming and livestreaming of child sexual abuse to industry transparency and reporting. Governments have partnered with the WeProtect Global Alliance — an international body comprising government, industry and civil society members — to promote the principles globally and drive collective industry action.

39. In almost two years since tech companies endorsed the Voluntary Principles, there is limited evidence as to the degree of implementation and the level of success. Given the rapid rise in CSAM available online and reports to NCMEC, it is important that tech companies work alongside government agencies, as well as bolster resources and capabilities, to keep pace with the proliferation of child sexual abuse offending on social media platforms.

40. Digital industry transparency reporting relating to online child sexual abuse is produced in an uncoordinated and inconsistent way. Comparable transparency reporting is key to understanding what companies are already doing to deter, detect and report CSAM and activity on their platforms and services. This will assist in identifying current gaps as well as provide qualitative and quantitative data to assist analysis of what is successful and where further efforts need to be focused.

41. Several countries and intergovernmental bodies are seeking to introduce mandatory transparency reporting as part of online safety legislation or industry codes. Australia's *Online Safety Act 2021*, which comes into force in January 2022, will include Basic Online Safety Expectations and industry Codes that will provide some level of regulation in this area.

42. The Technology Coalition has recently released its annual report in which it states that 71% of its members already publish regular transparency reports or will be doing so from this year. However, there is no best practice framework or benchmark for these reports. Representatives from Australia, UK, US, Canada and New Zealand have proposed that industry co-design a voluntary transparency framework to ensure consistent and informative data points. We still await a detailed response from industry on this proposal.

43. This lack of transparency prevents a true understanding of the scale of the threat, and impedes the development of legislative and regulatory responses, as well as remedies for victims of these crimes or abusive behaviours.

Government measures

44. The Australian Government continues to pursue a range of domestic and international initiatives to increase transparency and accountability of digital platforms, including through:

    - the National Strategy to Prevent and Respond to Child Sexual Abuse – which included $307.5 million to fund the first four years of a coordinated, whole-of-nation approach to preventing and responding to child sexual abuse in all settings, including ensuring criminal justice agencies have the necessary resources, tools and capabilities to detect, disrupt and prosecute this escalating threat;
    - regular strengthening of Commonwealth criminal law frameworks, including most recently the *Online Safety (Transitional Provisions and Consequential Amendments) Act 2021* and *Crimes Legislation Amendment (Sexual Crimes Against Children and Community Protection Measures) Act 2020*;
    - supporting international efforts including the G7 Internet Safety Principles, the recent G20 leader's declaration, and the US led Alliance for the Future of the Internet; and
    - research and awareness raising efforts, including the launch of 'Trace an Object' on 3 March 2021, as the Australian version of the 'Stop Child Abuse-Trace an Object' platform developed by Europol which encourages the community to identify objects from the background of images and videos containing sexually explicit material involving children.

Disinformation and misinformation

45. The development of modern communications technologies, social media and the internet have created opportunities to both strengthen and undermine Australia's social cohesion. The evolution of the global information infrastructure — particularly social media — has seen an increased spread of misinformation (false information that is spread due to ignorance, by error or mistake, with good intentions, or without the intent to deceive) and disinformation (knowingly false information that is spread to deliberately deceive, mislead, influence public opinion, or obscure the truth for malicious or deceptive purposes).

46. The increased prevalence of mis/disinformation in the digital environment poses a threat to the ability of Australians to make independent decisions, and erodes public confidence in our political and government institutions. The international nature of the most popular social media platforms and the importance of long-held democratic values of free and open expression however make moderation or regulatory responses complicated.

47. The Department remains committed to countering misinformation and disinformation that has the potential to undermine Australia's social cohesion. This includes referring instances of harmful misinformation to relevant agencies or to social media platforms for the platform's consideration for removal against their terms of service. Most recently, this has been focused on the spread of misinformation in relation to COVID-19. Between 16 March 2020 to 30 November 2021, 2842 instances of online COVID-19 misinformation were referred to digital industry for consideration against their terms of service.

Foreign Interference

48. Digital platforms, including social media applications, can be an effective tool for perpetrating foreign interference. Hostile foreign powers and their proxies are known to use digital platforms to promote narratives and/or spread disinformation that serves their strategic interests. This can include attempts to influence communities and broader public opinion on matters of importance to them, to undermine democratic processes and institutions, or stifle dissenting voices. The open nature of social media, where all users are free to express their own views (subject to platform terms of use) on political and social issues, irrespective of their expertise or credentials, provides an ideal environment through which to seed disinformation or otherwise spread inauthentic information and communications.

49. The Department refers the Committee to its submission to the Senate Select Committee on Foreign Interference through Social Media, which provides further details.

Violent extremism

50. Digital platforms present deep-seated challenges for Australia's national efforts to contest and prevent violent extremism. Increasingly, violent extremists from across the ideological spectrum seek to use online methods to spread extreme and harmful propaganda, seed division and recruit individuals. The Department limits terrorist and violent extremist groups' ability to exploit the internet for planning, fundraising, and communicating online, by undertaking actions to identify, analyse and counter terrorist and violent extremist use of digital platforms.

51. The Department's activities to limit the spread of terrorist violent and extremist content (TVEC) online includes working with major platforms to encourage the proactive identification and removal of extremist content through operational assistance, policy development and legislative obligation, including through the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* and the *Online Safety Act 2021*. The Department leads Australia's representation and participation on international forums and industry groups relating to TVEC on the internet, including the Global Internet Forum to Counter Terrorism. Complementary to work done by the eSafety Commissioner, the Department identifies and refers TVEC to digital platforms for consideration against their terms of service for removal. The Department also delivers strategic communication activities to undermine terrorist and violent extremist propaganda online by promoting positive alternative narratives and pathways to support a socially cohesive Australia.

52. Social media remains a major conduit for terrorism and violent extremist content. Although the Australian government and its international counterparts have taken steps to block or remove terrorist content online, there has been a notable shift by terrorist propaganda distributors from major online platforms towards more obscure and lesser known platforms that are either unwilling or unable to remove terrorist content.

Cybercrime

53. Cybercrime takes many different forms and includes both traditional crime types that are now cyber-enabled, and newer cyber-dependent crimes that are unique to the online environment. Social media platforms provide abundant opportunities for savvy cybercriminals through a range of well-known methodologies including but not limited to romance scams, catfishing, fake giveaways, buying or selling scams and phishing.

54. In 2020-21, over 67,500 cybercrime reports were made via the Australian Cyber Security Centre's ReportCyber portal. This was an increase of nearly 13 per cent from the previous financial year. Once reported to the relevant platform, the user profile is usually removed, however, it becomes a never ending 'whack-a-mole' game with new profiles and scams popping up regularly. There has also been an evolving trend of cybercriminals taking advantage of topical situations, such as the COVID-19 pandemic, to benefit from vulnerable victims.

Other matters

Collection and use of data

55. The Terms of Reference specifically request evidence regarding the collection and use of relevant data by industry in a safe, private and secure manner.

56. The Department notes that the widespread use of digital platforms has resulted in a vast trove of data on individuals and businesses that, in aggregate, is of high value to Foreign Intelligence Services. The Zhenhua Database (publicly available personal data compiled by a Chinese company) is but one example of the collection of personal information in a bulk data set. This issue underlines the importance of raising community understanding of how to act online in a secure manner. Everyone should be conscious of what information they post to the digital world, and how it can be 'scraped' and used. Social media companies should explore means of mitigating scraping and espionage on their platforms. More stringent requirements around consent should also be considered to ensure individuals are provided with every opportunity to limit the use and dissemination of their data. Further to this, services must not be withheld should an individual refuse consent to their data being used for non-service delivery purposes.

57. The Department is leading efforts to uplift data security policy settings across government and the broader economy, driven primarily through the National Data Security Action Plan (the Action Plan), an initiative announced by the Prime Minister in May 2021 as part of the Digital Economy Strategy.

58. The Action Plan will set out a comprehensive roadmap of measures to uplift data security across the broader economy. The Action Plan will take a phased approach to strengthen and coordinate data security policy settings across the Australian Government, state and territory governments and the broader economy. Key lines of effort under the Action Plan include:

    - clearly articulating the risk and geostrategic competition that surrounds the management, transfer, storage and security of data;
    - setting out the principles that Australian governments, organisations and individuals should consider to better protect data; and
    - reform options to improve data security across governments, businesses and the community.