

IQ23-000006

Division/Agency: Agency - eSafety Commissioner

Hansard Reference: Written, (20 February 2023)

Topic: eSafety - Risk associated with emerging immersive technologies

Senator Helen Polley asked:

eSafety provided evidence about risks associated with emerging immersive technologies (Submission 44, pp. 12–13; Proof Committee Hansard, 20 February 2023, pp. 22–23).

(a) Could you please provide more detail about the potential risks in relation to child sexual exploitation?

(b) What action could be taken now to mitigate these risks, such as requirements to embed safety by design principles?

Answer:

Similar to non-immersive online environments, emerging immersive technologies carry the risk of adults accessing, creating and sharing child sexual exploitation material, as well as making contact with children for the purposes of sexually grooming, exploiting and abusing them.

There are several factors which may contribute to these risks being heightened in emerging immersive environments.

Immersive technologies like virtual reality are capable of creating hyper-realistic experiences. Perpetrators may therefore be attracted to using these technologies to engage in child sexual exploitation. For example, reports have emerged in the UK of perpetrators using virtual reality headsets to view and store child sexual abuse material.¹ In addition, immersive multi-person environments that lack effective measures to separate children and adults can create a potential vector for grooming and sexual assault. Assault offences that were previously limited to the physical environment could be extended to the online environment and experienced in an intensely real way by the victim,² with lasting feelings of fear, anxiety and trauma.³

¹ A Crawford, *Child abuse material found on VR headsets, police data shows*, BBC News, 22 February 2023 <https://www.bbc.com/news/uk-64734308>.

² MA Lemley, E Volokh, *Law, virtual reality, and augmented reality*, SSRN Electronic Journal, doi:org/10.2139/ssrn.2933867, 2017.

³ JS Aubrey, MB Robb, J Bailey, J Bailenson, *Virtual Reality 101: What You Need to Know About Kids and VR*, Common Sense, 2018 <https://www.common sense media.org/research/virtual-reality-101-what-you-need-to-know-about-kids-and-vr>.

Infrastructure, Transport, Regional Development, Communications and the Arts

Committee Inquiries Question on Notice

Parliamentary Joint Committee on Law Enforcement

Inquiry into law enforcement capabilities in relation to child exploitation

These risks may be amplified by parents and carers being less aware of their children's activities in immersive environments. In addition to digital literacy gaps, it can be more difficult to see what a child is doing when they are wearing a virtual reality headset compared to when they are on a smartphone. Parents may also be less equipped to navigate safety and privacy setting given the nascence of these technologies.

With intentional planning and assessment of risks, providers of emerging immersive technologies can prevent and mitigate these harms. The foundational elements of how to do this are laid out in eSafety's [Safety by Design](https://www.esafety.gov.au/industry/safety-by-design) (<https://www.esafety.gov.au/industry/safety-by-design>) initiative, guided by three key principles:

Principle 1 - service provider responsibility. Providers should identify, assess and address safety risks in service design and provision. In immersive environments, this could include considering the heightened risks that immersive technologies and haptic devices that simulate touch can create for users. Providers should invest in robust, privacy-preserving age assurance measures and innovative moderation tools to identify and combat serious harm such as child sexual exploitation. Strong safety and privacy settings should be on by default for children.

Principle 2 - User empowerment and autonomy. Providers should work with their user community to design accessible and inclusive information and features they can use to stay safe. In immersive environments, examples include features that create personal space boundaries to prevent virtual assault, and measures that enable real-time reporting of abuse.

Principle 3 - Transparency and accountability. Providers should be transparent about risks and the measures they are taking to address them.

eSafety can require providers of immersive social media, gaming, messaging, dating and other types of apps and sites to report how they are meeting Australia's Basic Online Safety Expectations to improve transparency and accountability of these services, and incentivise improvements in safety.

In addition, users in Australia who encounter illegal and restricted online content or experience child cyberbullying, adult cyber abuse or image-based abuse on these types of services and apps can make a [report](https://www.esafety.gov.au/report) (<https://www.esafety.gov.au/report>) to eSafety. Whether regulatory action can be taken will depend on the circumstances. eSafety can provide advice and support on how to stay safe, including by drawing upon our immersive technologies guide [Immersive technology | Gift Guide | eSafety Commissioner](#) for parents and carers.

**Infrastructure, Transport, Regional Development, Communications and the Arts
Committee Inquiries Question on Notice
Parliamentary Joint Committee on Law Enforcement
Inquiry into law enforcement capabilities in relation to child exploitation**

IQ23-000007

Division/Agency: Agency - eSafetyCommissioner

Hansard Reference: Written, (20 February 2023)

Topic: eSafety - Exercising new powers under the Online Safety Act 2021

Senator Helen Polley asked:

Considering that eSafety is now exercising a range of new powers under the Online Safety Act 2021, are there resourcing or other administrative challenges for eSafety?

Answer:

Decisions about eSafety's budget and resourcing are a matter for government.

You can find more information about how eSafety allocates its resources in its annual report: [Australian Communications and Media Authority; Office of the Children's eSafety Commissioner Annual Reports 2015–16](#)