UNDERSTANDING INTERNET CONNECTED DEVICE RISKS TO PROTECT CHILDREN

By Darren Hamburger

1st Feb. 2023
Part 1 of 2

Understanding internet connected device risks to protect children.

By

Darren Hamburger

In 2022 Australia experienced significant data breaches such as but not limited to Medibank Private, Optus, TPG, Telstra and Bunnings which impeded the right for individual privacy. These data breaches demonstrated how vulnerable users of online connected devices, software and services are. If adults are vulnerable to online threats, what risks lay ahead for children and adolescents during their online use? This article will be the first of a two part series creating community awareness surrounding the risks children and adolescents may encounter while using internet connected devices; with the second part providing some helpful suggestions regarding how parents can increase children's online safety.

Everyday parents make decisions regarding how their children use electronic devices, such as allotted time for use and frequency; yet an interesting question to pose is how many of these parental decisions are made with internet vulnerability in mind? Common parental decisions surrounding children's device use may typically be influenced by various circumstances I.E past experiences, schooling tasks, game play, interaction with friends or family and perhaps certain community norms. However, the premise of this article is that it's safer to assume all online activity should not be considered risk free. This is not to say internet connected device use should not occur; only that parents need to increase their understanding of the potential risks children may experience. Only with greater understanding will parents be in a better position to mitigate against vulnerabilities to keep children safe.

If we are to accept the premise that online activity carries certain risks to children's wellbeing; the next logical question is what are these risks? A study by Panhans et al. (2022) conducted a survey of 41,000 parents and children finding approximately 93% of the children surveyed who used the internet were between ages 8 to 17[1]. More importantly at least one cyber-threat was experienced by 73% of the children surveyed. The cyber-threat risks identified were placed into categories such as unwanted pop-ups and advertisements 47%, witnessing inappropriate images and other content 36%, experienced some from of bullying and harassment 19%, unwanted sexual approaches 17% and hacking, phishing or being sent viruses 17%.[1]

Online Content:

Content is one segment of online activity parents will need to consider monitoring to ensure satisfactory and safe viewing content for their children, especially if the media is derived from unregulated sources. Garlen & Hembruff (2021) cited a study by Auxier et al. (2020) reporting on a daily basis, 53% of the children were watching YouTube.[2] This is quite a large number of children's online content which is fuelled by content monetisation strategies.

However even more alarming was the historic occurrence of significantly disturbing material which had been found embedded within certain YouTube content subjecting children to distasteful content. In fact Garlen & Hembruff (2021) cited information by Maheshwari (2017) who provided two examples of inappropriate content for children which bypassed content filters on YouTube; stating "One example of these disturbing videos showed puppy characters from a popular animated preschool television called PAW Patrol committing suicide, with one walking off a roof after being hypnotised by a demon-possessed doll from an adult horror movie (Maheshwari, 2017). Another example was a video in which a clay caricature of the comic superhero Spider-Man is shown urinating on the character Elsa from Disney's popular animated *Frozen*."[2]

Bullying:

Bullying face to face or via online is a behaviour which has drawn much attention over the years because of how tremendously damaging it is to victims. Sun Hong et.al (2019) defined bullying as being ‘characterised by the repeated exposure of one person to physical and / or emotional aggression including teasing, name calling, mockery, threats, harassment, taunting, hazing, social exclusion or rumors’.[3]

In their study, Baier et al. (2019) identified psychological cyberbullying was reported the most frequent in both male and female students. While types of bullying such as relational and cyberbullying were the most highly correlated forms of bullying. Sexualised cyberbullying containing gender based harassment, sexual comments and sexual assault impacted girls mental health was identified; while males were not seen to experience sexual harassment. [4]

Bullying wields significant and often long term injury to the victim. In their study, Ford et al. (2017) confirmed the association of depression, anxiety, suicidal ideation, self harm, suicide attempt and suicide as a result of bullying injury, which included being a “Victim” or “Bully-Victim”. For clarity the ‘bully-victim’ is an individual who has experienced being bullied and also has bullied others.[5] Thulin et al. (2022) found mental health significantly impacted schooling performance, resulting in lower grades; while also finding depression and somatisation resulted from bullying.[6]

Mental Health

Baier et al. (2019) cited a study by O’Keeffe et al. (2011), highlighting extended amounts of time using social media is likely to reinforce negative outcomes such as Anxiety and Depression.[4]

We also know historically ‘Facebook’ previously conducted a questionable experiment authored by Kramer et.al (2014); to alter user mood states without expressed consent to that particular study. Facebook during their experiment manipulated news feeds of 689,003 Facebook users without their knowledge and sought to specifically alter peoples emotional states.[7] This Facebook experiment demonstrates social media platforms can be dangerous whereby deceptive algorithms and organisational interest take precedence overlooking ethical standards affecting our emotional states without our knowledge; while simultaneously altering factual information shown to us in order to produce a certain influence or false belief. Secondly, this experiment demonstrates social media platforms have the capacity to use data in ways that most social media users may not necessarily expect regardless of the typical overreaching broad consent provided at first account setup. Finally, vulnerable populations such as children and adolescents can quite easily be negatively influenced having absolutely no understanding how their beliefs could be altered. To further highlight the nuances of commercial interests, Fortnite is another example where commercial interests were superimposed over the well being of its users. In 2022 Fortnite a free to download game was fined in total $520 million due to using “privacy-invasive default settings and deceptive interfaces that tricked Fortnite users, including teenagers and children,"[8] while placing “children and teens at risk through its lax privacy practices, and cost consumers millions in illegal charges through its use of dark patterns,”[8]

The two examples provided here highlight the potential to affect mental health either directly or via indirect harms. Therefore something seen to be free of charge and popular does not necessarily mean parents should automatically assume the child will be safe. One thing is for certain, there are free to use programs and apps available which on the surface appear harmless, however attempt to influence the user to spend money which is a similar commercial interest tactic employed no different to gambling advertisements inciting persons to gamble causing multiple forms of harm. “Responsible gambling”… there is no such thing.

Electronic Dating Violence

As adolescents continue to develop towards the path to adulthood; it's only natural social interaction, independence and sexuality will continue to become topics of greater focus. Thulin et al. (2022) reported electronic dating increased during the adolescent phases while age 16 was typically an average first exposure.[6] Thus electronic dating violence is another online risk adolescents may at some point experience. Behvaioural risks which surround electronic dating violence are attempts to control the victim; an ability to easily share private information en-mass; the creation of fake accounts or deceptively connect with the victims social media accounts in order to be able to access additional information which subverts the victims attempts to separate from the offender. This effectively avoids being removed or being blocked from information when the victim attempts to sever communication. The final element identified was experiencing great difficulty removing unwanted publicly viewed information is likely to produce additional re-traumatisation to the victim. [6]

In their study, Thulin et al. (2022) identified electronic monitoring behaviours had continually escalated from age 12 through to age 18. Harassment and coercion continually escalated from age 12 right through to 16 and then retracted slightly till age 18.[6] The overall conclusion of these findings demonstrate children even while ageing into late adolescents still required additional parental support regarding their child's online activity. However social supports were positively linked with improved mental health outcomes, especially in girls.[6]

Illicit Substances

Communication is perhaps one of the more common reasons online connected devices are used; employing a broad range of methodologies such as online web chats, social media interaction, using communication apps, e-mail, text messages and of course the humble telephone call. Unfortunately apps maybe used in certain ways not intended by their developers; while children and adolescents risk being subjected to illicit substances traded online. In their study Sullivan & Voce (2020) identified a vast number of social media and messaging apps which had been used during the sale, purchase and distribution of illicit substances of detainees. The leading messaging app used was Facebook messenger, following Wickr, Snapchat, Whatsapp, iMessage, Signal, Skype, Kik, Facetime and Viber.[9]

Development

Hamburger (2022) cited the Hosokawa & Katsura (2018) study which examined mobile technology use and adjustment in 5 year old's which identified increases of hyperactivity, inattention, conduct problems and emotional symptoms. These behavioural difficulties were significantly linked to regular use of mobile devices in 14% of the participants who use electronic devices 60 minutes or more of the day.[10]

Of particular interest to this article, the 'Hosokawa & Katsura study cited additional studies which also identified numerous other adverse impacts to child development as a result of excessive electronic device use, such as social and psychological development, reducing parental-child interaction, impeding furthering development of associated verbal learning, problem solving and expressive creativity, sleep disturbance, lowered physical fitness and increased isolation which restrict social interaction cues development.'[11]

Software

Of course one major component to online safety is the software developed for device users to download and install. Given majority of device users are not skilled in software development and design, each device user is beholden to trustworthiness of its software developers. In 2022 The Humans Rights Watch Organisation provided an extensive report highlighting various educational software on devices harvested certain personal data specific to device ID without people knowing. [12] The use of child educational programs during the Covid-19 pandemic, escalated the demands for

children to have internet connected devices; and in some cases schools will stipulate which devices or software are to be used. However if schools undertake such demands upon their students, the schools should essentially take all actions to investigate and ensure the safety and privacy of such software, the origin where data is held, which data is collected and child and parents are well informed of how data is used and stored prior to children using the software.

Conclusion:

This article recognises that a large proportion of children use internet connected devices which carry certain risks. The risk of harm domains discussed within this article are online dating violence, inappropriate content being published, introduction to illicit substances, bullying, impacts on mental health and development and software privacy.

This article also brings to light that nefarious actors online are not just the typical ‘hacker’ ideology; in fact online nefarious actors can quite easily become a friend, a family member, persons we interact with by association, in addition to those within the online community who seek to deliberately exploit persons for their own gratification.

This article simply acknowledges that children and adolescents online are subjected to risks, however is not advocating children don’t use electronic devices. The main purpose of this article is to highlight potential risks and that it’s important care givers have a proactive approach to understanding and monitoring children's online activity; especially the type of software used while taking the necessary actions to mitigate risks.

References

[1] D. Panhans, S. Yousuf, A .Alfaadhei, L. Hoteit, T. Breward, B. H. (2022) Why children are unsafe in cyberspace,. Alshaalan. *Boston Consulting Group,* Global Cybersecurity Forum p 1- 10

[2] J. Garlen, S. Hembruff (2021), Unboxing Childhood: Risk and Responsibility in the Age of YouTube. *Journal of Childhood Studies*. Vol. 46 No.2 p78-90

[3] J. Sung Hong, D. L Espelage, C. A Rose (2019) Bullying, Peer Victimisation and Child and Adolescent Health: An Introduction to the Special Issue. *Journal of Child and Family Studies*. 28 pp 2331-2334

[4] D. Baier, J. S Hong, S. Kliem, M. C Bergmann (2019), Consequences of bullying on adolescents' mental health in Germany : comparing face-to-face bullying and cyberbullying. *Journal of Child and Family Studies* 28: pp2347-2357

[5] R. Ford, T. King, N. Priest, A. Kavanagh (2017) Bullying and mental health and suicidal behvaiour among 14 to 15-year-olds in a representative sample of Australian children. *Australian & New Zealand Journal of Psychiatry*, Vol 51 (9) p 897-908

[6] E. Thulin, M. A. Zimmerman, Y. Kusunoki, P. Kernsmith, J. Smith-Darden, J. E. Heinze (2022) Electronic Teen Dating Violence Curves by Age. *Journal of Youth And Adolescence*. 51. pp45-61

[7] A. Kramer, J. Guillory, J. Hancock (2014), Experimental evidence of massive-scale emotional contagion through social networks. *PNAS* Vol.111 No.24 pp8787 - 8790

[8] (2022), Fortnite Video Game Maker Epic Games to Pay More Than Half a Billion Dollars over FTC Allegations of Privacy Violations and Unwanted Charges. *Federal Trade Commission*. https://www.ftc.gov/news-events/news/press-releases/2022/12/fortnite-video-game-maker-epic-games-pay-more-half-billion-dollars-over-ftc-allegations

[9] T. Sullivan, A. Voce (2022) Statistical Bulletin 22: Use of Mobile Phone to buy and sell illicit drugs. Australian Institute of Criminology: Australian Government pp 1-10

[10] D. Hamburger (2022) Does too much electronic device use really impact child & adolescent development? *www.darrenhamburger.au* pp 1-4

[11] R. Hosokawa, T. Katsura (2018), Association between mobile technology use and child adjustment in early elementary school age. Plos ONE 13(7):e0199959. p1-17

[12] Humans Rights Watch (2022), How dare they peep into my private life? Children's Rights Violations by Governments That Endorse Online Learning During the Covid-19 Pandemic. *Humans Rights Watch*. p1-100