Online Safety Act Review Submission

June 21, 2024

Table of Contents

Online Safety Act Review Submission

Part 2 question 1

The current wording for the Online Safety Act 2021 section 134 (h) doesn’t cover Internet of Things (IoT) in an obvious way. The definition of “relevant electronic service” pertains to direct communication between one user and another, however indirect communication and IoT devices that broadcast a signal can also be used for monitoring and stalking. Examples include using the Messenger and WhatsApp app interface tells you the last time someone was seen online, or surreptitious installation of a GPS tracker in the target’s belongings (Stevens et al., 2021). IoT devices often collect personal information, which, combined with poorer security practices than for other computing equipment, makes them fertile ground for exploitation even for a low-ability attacker. The Online Safety Act should mention IoT because IoT devices are often interconnected with mobile phones, controlled by them, and specifically designed to require less technical expertise to deploy (Slupska & Tanczer, 2021). Additionally, IoT major appliances that are installed in the home such as air conditioners, security cameras and door locks, if they were purchased and installed by a domestic partner or housemate that leaves on bad terms, are a tech abuse risk. Potential abuses include remotely adjusting product settings on the airconditioner to cause large power bills for the house occupant, monitoring house occupants using camera footage or unlocking a smart lock to leave a house vulnerable to burglary. In cases of installed IoT devices, the courts should be able to compel the manufacturer to reset the IoT device permissions to give control to the house occupant as they do in the UK (Slupska & Tanczer, 2021).

Part 6 question 29

In answer to the Issues Paper question 29, I have taken the same technology-neutral approach like the World Economic Forum (2023) to explain emerging online harms in this submission. Legislative challenges exist with naming specific technology-related offences, which is particularly difficult with respect to the inventiveness of offenders executing technology-enabled abuse (O'Shea et al., 2022; Powell & Henry, 2018). If there was a statutory duty of care or Safety by Design obligation, it would not change my answer because naming specific technologies is always going to be a step behind the many ways people intent on punishing a target find a way to misuse technology to achieve that purpose.

Before defining a duty of care or safety by design obligation, quite a lot more work has to be done to connect the research into online harms published by criminology or sociology researchers and the cybersecurity community. In doing background research for this submission, I also discovered that cybersecurity industry operational resources such as the Mitre Corporation's "Att&ck" and "D3fend" websites (https://attack.mitre.org/matrices/enterprise/ and https://d3fend.mitre.org/) include very little information to raise awareness about technology-facilitated abuse. A search of Mitre Att&ck techniques that could pertain to technology-facilitated abuse includes "trusted relationship" (where the attacker has administrative privileges in the home network or technology, see https://attack.mitre.org/techniques/T1199/). All the examples are from hacker groups (state-sponsored or otherwise), or "gather victim information", that has only one mitigation listed (see - https://attack.mitre.org/techniques/T1589/), which is relevant to an organization's IT team, not a consumer. Other tech abuse relevant to low-tech attack methods include installing malicious browser extensions, or accessing default accounts (https://attack.mitre.org/techniques/T1176/, https://attack.mitre.org/techniques/T1078/001/), not all of which are within scope of a target with little technical expertise.

Slupska and Tanczer (2021) have attempted to define a threat matrix that focusses on "UI-bound attackers", instead of the usual criminal commercial enterprises and state-sponsored actors found on the Mitre corporation sites. This is a good start to pose a series of questions that app developers must consider before launching their software. An example would be asking software developers to consider ethical questions such as whether the app/program's method of implementing access controls maintains human dignity, autonomy and the common good (Schreider & Noakes-Fry, 2020) from the perspective of authenticated users, with one user being hostile to another user. It would be a good idea if the duty of care requirement included some way to have new tech devices independently tested, to confirm there is no way to send harmful messages, access someone else's personal information or engage in gaslighting behavior using it (Slupska & Tanczer, 2021). Using a traditional penetration tester may not work in this scenario as the assumption is that the attacker is technically proficient at hacking. This contradicts with Slupska & Tanczer's (2021) assessment of UI-based attackers, so the service contract with the penetration testing service would at minimum have to include the definition of a UI-based attacker in the scope of works to effectively test software for tech abuse vulnerabilities.

Part 6 question 30

Existing criminal law covers stalking/cyberstalking in domestic relationships only, which fails to acknowledge stalking in any form can be perpetrated by a stranger(s). The Issues Paper mentions celebrities and public figures, but there are other examples of intrusive monitoring that intrude on a person's privacy. These scenarios do not fall under the Australian Privacy Act 1988 because the intrusive monitoring isn't being conducted for government or private sector service delivery. Therefore, the Online Safety Act wording should include protection for any individuals being intrusively monitored by strangers, not just public figures and celebrities. Some specific scenarios from personal experience include:

- Someone from my past moved into a new house and discovered that it came with its own stalker. The stalker had no relationship to the family living in the house, but would leave gifts and notes on the back doorstep addressed to someone not known at the address. Taking or not taking the “gifts” inside did not stop the behaviour. Given the family had just had their first child, it was concerning for the husband to go to work each day, in his mind leaving his partner and child undefended with no understanding of the stalker’s endgame. In the end, the family had to install CCTV at their own expense to catch the offender. The police charged the offender with trespassing, and although this time the family had the financial resources to install CCTV, not everyone has the means to defend themselves like this. It would limit the Online Safety Act’s utility if it was written from the perspective of assuming every target has resources and ability to go after their attacker.
- Many years ago, I tried to help a veteran with some simple mental health tools I had experience using, but, lacking in personal boundaries, he took to phoning with his phone set to no caller ID. I explained to him repeatedly that I did not have the professional training to tackle his problems, but he still rang often and would let it ring out when I didn’t pick up the phone. If I didn’t answer, he would ring again a couple of times immediately after. I went to the police after the stress made me

succumb to a cold and was told that the police couldn’t do much more than go and talk to him.

Part 6 question 31

The societal belief is that hate speech is a byproduct of hateful people (Munn, 2020), when really what is happening is that the privilege of internet anonymity is being used to give voice to morally repugnant attitudes that people wouldn’t admit to offline. Section 7 (1) subpart C of the Online Safety Act 2021 does not acknowledge the full range of online harms, such as the ability of coercive control to be used for blackmail, distributed intrusive monitoring or inciting others to commit crimes. The existing adult cyber-abuse section in the Online Safety Act doesn’t have coverage for stranger stalking or third party attacks. In cyber law, intrusive monitoring or calling for others to be attacked is a type of inchoate crime (Schreider & Noakes-Fry, 2020). With tech abuse scenarios, the person with intent to harm might do the monitoring themselves but call for others to complete the attack. Alternately, they crowdsource the monitoring to determine the best time and place for a physical attack, then complete the crime themselves (Schreider & Noakes-Fry, 2020). Examples of this type of third-party attack are mentioned by Powell and Henry (2018):

- A domestic violence survivor reported to the police that her ex-partner had put her details up on craigslist is a provider of sexual services. The ex-partner misrepresented the victim to other computer users, resulting in them making phone calls to the victim. They were unknowingly harassing this woman on behalf of her ex-partner. This scenario couldn’t be prosecuted as domestic violence. What is important to third-party attacks is that an ex-partner avoids attacking directly to get around existing domestic violence protections like non-contact orders.

- Use of discussion boards for individuals to gather and amplify repugnant attitudes, such as a “where are they now” facebook group being used to re-identify now-adult child abuse survivors for the purpose of trolling them.
- Distributed information-gathering or offending, such as requesting that someone be raped or for information to facilitate someone to be blackmailed, where the attacker’s intent could be to avoid a non-contact order or to discourage the target contacting law enforcement.

References

Munn, L. (2020, July 30). Angry by design: Toxic communication and technical architectures. *Humanities and Social Science Communications, 7*, Article 53.

O'Shea, B., Asquith, N.L., & Prichard, J. (2022). Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking. *International Journal for Crime, Justice and Social Democracy*, *11*(4), 25–39. https://doi.org/10.5204/ijcjsd.2096

Powell, A. and Henry, N. (2018). Policing technology-facilitated sexual violences against adult victims: police and service sector perspectives. *Policing and Society, 28*(3), 291-307. https://doi.org/10.1080/10439463.2016.1154964

Schreider, T., & Noakes-Fry, K. (2020). *Cybersecurity law, standards, and regulations* (2nd ed.). Rothstein Publishing.

Stevens, F., Nurse, J.R.C, Arief, B. (2021, June 14). Cyber stalking, cyber harassment and adult mental health: A systematic review. *Cyberpsychology Behaviour, and Social Networking, 24*(6), 1-19. https://doi.org/10.1089/cyber.2020.0253

Stevens, T. (2021). *United Kingdom: Pragmatism and adaptability in the cyber realm*. In Romaniuk, S. N. & Manjikian, M. (Eds.), Routledge companion to global cyber-security strategy, (pp. 191-200). Taylor & Francis.

World Economic Forum. (2023, August). *Toolkit for digital safety design interventions and innovations: Typology of online harms.* https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf