CASA Forum
Victorian Centres Against Sexual Assault

The Victorian CASA Forum submission to Australia’s 2020 Cyber Security Strategy

The Victorian CASA forum welcomes the Australian Government's decision to develop our nation’s next Cyber Security Strategy as part of its commitment to protecting Australians from cyber threats. We are pleased to put forward our submission to the Department of Home Affairs and the Australian Signals Directorate’s Australian Cyber Security Centre.

About the CASAs

The Victorian CASA Forum is the peak body for the 15 Centres Against Sexual Assault (CASAs) in the State. Fourteen of these Centres provide direct services. The other Centre is the Sexual Assault Crisis Line (SACL) which provides an after-hours telephone response. Six of the CASAs are based in metropolitan areas. One of them is based at the Royal Children’s Hospital, the Gatehouse Centre and sees children, adolescents and their parents or carers. The other eight CASAs are based in regional areas of Victoria.

About sexual violence

Sexual violence includes two key components: sexual assault (acts of a sexual nature carried out against a person’s will, and which would be considered an offence under state and territory criminal law), and sexual threat (the threat of acts of a sexual nature that are made face-to-face where the person believes it was able to and likely to be carried out).

Statistics on sexual violence

Approximately one in five women (18% or 1.7 million) has experienced sexual violence (the occurrence, attempt or threat of sexual assault) [1]

One in six women (17% or 1.6 million) has experienced an episode of stalking (any unwanted contact or attention on more than one occasion, or multiple types of unwanted contact or behaviour experienced on one occasion, that could have caused fear or distress). [1]

Approximately one in four women (23% or 2.2 million) has experienced emotional abuse by a partner. [1]

About family violence

The Commonwealth Family Law Act 1975 defines "family violence" as "violent, threatening or other behaviour by a person that coerces or controls a member of the person's family, or causes the family member to be fearful".

Statistics on family violence

One in four women have experienced at least one incident of violence by an intimate partner.

Regarding their most recent incident most women:

- reported that the incident happened in their home;
- did not perceive the incident as a crime;
- experienced fear or anxiety after the incident; and
- did not take time off work as a result of the assault. [2]

1 What is your view of the cyber threat environment?

The current cyber threat environment needs to be expanded to include the threat of technologically facilitated abuse, particularly in relation to sexual violence and those in a family violence situation.

Internet enabled devices are already being used to stalk and monitor current or ex-partners.

“These include sending abusive text messages or emails, making continuous threatening phone calls, spying on and monitoring victims through the use of tracking systems, abusing victims on social media sites, and sharing intimate photos of the victim without their consent (“revenge porn”).” [3]

Sexual and family violence often includes privacy violations such as surveillance, monitoring, or other stalking. For a sexual or family violence victim, privacy in relation to their activities goes hand in hand with their physical safety. These activities might be seeking information about how to escape from an abusive relationship, electronically storing evidence of abuse or critical documentation as part of a safety plan.

Perpetrators use mobile technologies to create a sense of being ever-present in the victim’s life. Fraser et al. writes that “one of the more terrifying tactics used by stalkers is to make the victim feel that she has no privacy, security, or safety, and that the stalker knows and sees everything.” [4]

1b What threats should Government be focusing on?

The government should be focusing on introducing systems that ensure the safety of women and children against abusive partners or ex partners, who are using technology to harm, intimidate, stalk or monitor them.

5 How can Government maintain trust from the Australian community when using its cyber security capabilities?

To maintain trust from the Australian community, we recommend that the government ensure there is some form of declaration that all workers with any access to personal information must sign to say that states that neither they, nor any member of their family, or any close friend or associate of theirs:

- has had any allegations of sexual or family violence made against them
- have never had an intervention order taken out against them.
- are not on the sexual offenders register
- have never been charged with any form of sexual violence or family violence

This is because statistics show that family violence in Australia affects 1 in 4 women and 1 in 5 women has experienced sexual violence. A percentage of these women will be in a relationship with, or have a connection to the men and women who make up the “officers and authorities of the Commonwealth and of the States and Territories” who are in charge of monitoring activity, storing data or enacting cyber security legislation. The government would need to ensure that there are checks or balances in place to stop current or ex partners who are in these positions, or know or are related to someone in these positions, from using devices or the data collected against victims.

As the case involving Senior Constable Punchard [5] illustrates, at the very least there needs to be education for this worker population so they properly understand their duty of care and the potentially deadly consequences their actions could have for someone in a sexual or family violence situation.

6 What customer protections should apply to the security of cyber goods and services?

- There needs to be regulation and accountability by manufacturers about the security of internet enabled devices.

A range of things like mobile phones, social networks and the IoT offer a whole new spectrum of ways in which technologies with legitimate purposes are turned into ways of perpetuating violence against women and children.

“As we continue to see the exponential growth of internet of things devices, we will continue to see security issues we hadn’t even considered before.” [6]

The security and privacy of consumer technology must be raised to bring it into line with other everyday items such as cars, food and toasters.

7 What role can Government and industry play in supporting the cyber security of consumers?

- There should not be a default login encoded into devices.
- There must be an automated way for security updates to be installed on devices.
- There must be a simple way for the owner to check who has accessed the device.
- There should be consumer education on how to protect privacy and make a device secure
- There should be free access to a helpdesk to take devices to or to consult if a person suspects their device has been compromised.
- Connected vehicles should have advanced technologies like secure boot to ensure the integrity of the vehicle is intact. They should be rebooted every service.
- There should be extensive and ongoing technology training for anti-domestic violence and sexual assault practitioners about how to respond to and prevent technologically facilitated violence.

10 Is the regulatory environment for cyber security appropriate? Why or why not?

- We do not believe the regulatory environment for cyber security is appropriate as it currently stands.
- Legal protections need to keep pace with technological development, and be meaningfully enforced. These should include privacy breaches and the misuse of private information such as intimate images. Example: It is hard to get an image deleted from a social network.
- Most current options, such as an apprehended violence order, were created to protect the victim from physical contact. They do not protect against electronic monitoring or stalking.
- Greater penalties are needed for technologically facilitated abuse

11 What specific market incentives or regulatory changes should Government consider?

- We would recommend that government consider a security rating system so that people will understand how secure their device is before they buy it.

For those who do not have either direct physical access to a device or knowledge of passwords, Internet of Things (IoT) devices are notoriously insecure and easy to hack. The prevalence and severity of using technology like phones and computers for violence against women is well documented.

A woman bought a webcam and within a short time “the camera started following me back and forth and …then I heard, 'bonjour madame.' I yelled, "Get the f*** out of my house." "Hola señorita," the hacker teased. "Suck my d***!" [7]

- There needs to be greater Police education on the issue of sexual and family violence and technology and how to best respond.

There is often a disconnect between the general law enforcement (as opposed to specially trained units) and some types of sexual and family violence. Victims have described how police have accused them of having mental health issues when they complain that their home is bugged or that there have been changes to online accounts that they did not make.

Another of our concerns is that using IoT devices to stalk and monitor will make this more pronounced. It will be difficult for a victim to explain and substantiate that her ex is using her power consumption records to monitor when she is at home. We also envisage that law enforcement will be perplexed as to how to respond to such an allegation, let alone understand how to stop this.

- We would like to see more funding put into support programs such as the ‘Safe at Home’ initiative that checks houses for electronic surveillance devices free of charge to the victim.

12 What needs to be done so that cyber security is ‘built in’ to digital goods and services?

They need to be designed using ‘Secure by design’ practices.

22 To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

It is not just about being cyber aware. A consumer who wants to have the utmost security on her device is left to do her own research on how secure the firmware etc on a device is. Unlike other consumer goods, such as a pram for a child, there are no government standards or rating systems on technology goods other than perhaps an energy rating.

There seems to be a disconnect between manufacturers and developers to accept that they share the responsibility in finding solutions and enacting safeguards when their technology is used for sexual and family violence. In a number of high profile cases which centre on technologically being used for abuse (Gamergate, Twitter, Uber) there has been a lacklustre response from industry and authorities. When devices, platforms or applications are inherently used for sexual or family violence, no amount of cyber awareness is going to help consumers to be safer. That is like saying the passengers on the Titanic would have survived if they had swimming lessons.

25 Would you like to see cyber security features prioritised in products and services?

Yes

26 Is there anything else that Government should consider in developing Australia’s 2020 Cyber Security Strategy?

Family violence has killed more women in Australia than terrorism. For family violence victims, privacy is closely linked to safety. In Australia, one woman per week is killed from family violence. There needs to be standards and rating systems on all internet enabled devices to allow consumers to make informed choices.

There need to be education in law enforcement on how to deal with victims of technologically facilitated abuse.

The focus for cyber security needs to be broadened out to include victims of technologically facilitated abuse and not just focusing on business or economic issues.

References

1. Australian Bureau of Statistics. (2017). Personal safety, Australia, 2016. Canberra, ACT: Author. Retrieved from: http://www.abs.gov.au/ausstats/abs@.nsf/mf/4906.0

2. Violence against women: Additional analysis of the Australian Bureau of Statistics’ Personal Safety Survey, 2012. Retrieved September 25, 2019, from https://www.anrows.org.au/publication/violence-against-women-in-australia-additional-analysis-of-the-australian-bureau-of-statistics-personal-safety-survey-2012/

3. Al-Alosi, H. (2017, March 27). Technology-facilitated abuse: the new breed of domestic violence. Retrieved September 25, 2019, from http://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683

4. Fraser, Cynthia, Olsen, Erica, Lee, Kaofeng, Southworth, Cindy & Tucker, Sarah (2010), 'The New Age of Stalking: Technological Implications for Stalking', Juvenile and Family Court Journal, vol. 61, no. 4, pp. 39-55.

5. Siganto, T., & Robertson, J. (2018, December 17). Policeman stood down over "leaking" of DV complainant's address to former partner [Text]. Retrieved September 25, 2019, from ABC News website: https://www.abc.net.au/news/2018-12-17/brisbane-cop-stood-down-charged-for-leaking-womans-address-dv/10628106

6. Fearn, N. (2017, February 12). The internet of things can be hacked – and the risks are growing every day. Retrieved September 25, 2019, from http://www.techradar.com/news/the-internet-of-things-can-be-hacked-and-that-puts-your-life-at-risk

7. Jones, R. (2017, October 6). Woman's Webcam Starts Following Her Movements And Taunts "Hello." Retrieved September 25, 2019, from https://www.gizmodo.com.au/2017/10/womans-webcam-starts-following-her-movements-and-taunts-hello/

Karen Hogan
[redacted]
For the CASA Forum