MonashHealth

South Eastern CASA
Centre Against Sexual Assault & Family Violence

Wednesday 24th January 2018

To whom it may concern

Attached is a submission to the Enquiry into the Impact of New and Emerging Information and Communications Technology (ICT) by the Parliamentary Joint Committee on Law Enforcement.

This submission is made by the South Eastern Centre Against Sexual Assault and Family Violence (SECASA). We appreciate the committee's time and consideration of this topic and are happy to participate further should the need arise.

Please contact me if you need more information about SECASA's submission.

Yours faithfully

Carolyn Worth AM
Manager
SECASA

MonashHealth

South Eastern CASA
Centre Against Sexual Assault & Family Violence

Submission to the Joint Enquiry into New and Emerging ICT

This submission focuses on the challenges facing Australian law enforcement agencies arising from new and emerging ICT. In particular it highlights the role of the Internet of Things (IOT) in family violence related to:

1. Challenges facing Australian law enforcement agencies arising from new and emerging ICT;
2. The ICT capabilities of Australian law enforcement agencies.

About the CASAs and SECASA

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.

The South Eastern Centre Against Sexual Assault and Family Violence (SECASA) provides sexual assault and family violence services in Victoria within the Mornington Peninsula, Frankston, Bayside, Port Phillip, Stonnington, Glen Eira and Kingston local government areas. SECASA provides services to children and adults, both female and male, who have been sexually or physically assaulted. The Centre also works with non-offending family members, partners, caregivers and support workers. SECASA is a member of the Victorian Centres Against Sexual Assault (CASAs), which is a collective of non-profit, state-government funded rape crisis centres.

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". (Reference 1)

Family violence is when someone behaves abusively towards a family member. It is part of a pattern of behaviour that controls or dominates a person and causes them to fear for their own or others' safety and wellbeing.

Violent and abusive behaviour includes physical and sexual violence, and financial, emotional and psychological abuse. Slapping, hitting, rape, verbal threats, harassment, stalking, withholding money, and deliberately isolating someone from their friends and family are some examples of the types of behaviour that occur in family violence. (Reference 1)

Family violence and women and children

While every woman's experience of family violence is unique, for many women experiencing family violence there is a spiral of increasing abuse (this could be physical, emotional, financial, or a combination), rather than a one-off incident. Family violence often starts with an intimate partner's apparent love transforming into controlling and intimidating behaviour.

Over time, the woman is often increasingly isolated from friends and family by her partner. Physical violence may not occur until the relationship is well established, or it may not occur at all. The abusive, violent and controlling behaviours create an environment of fear and constant anxiety in a place where women and children should feel safe and secure. (Reference 1)

Family violence statistics

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. (Reference 2)

"Intimate partner stalking is a form of coercive control. Coercive control includes tactics not traditionally viewed as "serious forms of abuse". These tactics include strategies to control and intimidate, such as isolating the victim, surveillance and threats of violence. (Reference 6)

Family violence also includes emotional abuse. Emotional abuse is "behaviours or actions that are aimed at preventing or controlling (a partner's) behaviour with the intent to cause them emotional harm or fear".

Over 2.1 million women in Australia had experienced at least one incident of emotional abuse by a former or current cohabiting partner since the age of 15: this is one in four women in Australia (24.5%).

Approximately 1.8 million women reported that they had experienced emotional abuse from a partner they were no longer in a relationship with: this is one in five women in Australia (1,840,600, 21.1%).

Three out of four women had experienced anxiety or fear due to emotional abuse by a former cohabiting male partner (1,382,600, 76.3%). (Reference 2)

Internet of Things (IOT) and family violence

Internet enabled devices are already being used in family violence situations to stalk and monitor current or ex-partners. "These include sending abusive text messages or emails, continually making 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")." (Reference 3)

We are concerned that the new Internet of Things (IOT) trend will allow more ways for someone to stalk and/or monitor an ex or current partner. While people are becoming more aware that spyware can be installed on things like computers or phones, who would think that someone could be monitored via their fridge?

"An abusive ex-partner who still has remote access to his target's smart fridge might notice that she is suddenly stocking beer, which she never drinks. The abuser might leap to the conclusion that there is another man in her life, leading to an escalation of his behaviour—with potentially violent or even fatal consequences.

"The problem is that most people don't think like a psychopath. (Industry) makes these things and doesn't think about other ways in which it could be used." (Reference 4)

Using these devices an abuser could gather knowledge of a victim's day to day activities and personal habits remotely. This could be a powerful tool for coercive control and emotional abuse.

Take fitness wearables. These devices record biometrics and they are ideal surveillance devices because the device monitors when it is taken off, and a stalker can monitor the device. Currently if someone knows their phone is being tracked, they can leave it somewhere innocuous while they access a domestic violence service or women's shelter. Suspicion may be triggered if a fitness device is being tracked and the stalker can see when it was taken off, and for how long. (Reference 4)

Violence against women using the Internet of Things (IOT)

For those who do not have either direct physical access to a device or knowledge of passwords, IOT devices are notoriously insecure and easy to hack. The prevalence and severity of the use of 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***!" (Reference 5)

The IOT trend will offer a whole new spectrum of ways in which devices with legitimate purposes are turned into ways of perpetuating violence, particularly against women and children.

Trying to stay safer

"As we continue to see the exponential growth of the Internet of Things devices, we will continue to see security issues we hadn't even considered before." (Reference 7)

How does someone prove that their IOT device is being monitored? To detect this, and then gather evidence of it, a victim would need a sophisticated knowledge of technology. They would need to:

- Detect that a device has been compromised
- Capture evidence to document what was happening
- Find some way to show who has compromised it.

Only after these steps have been taken would law enforcement be able to act.

Searching the internet for information on what do to if you think you are being stalked usually gets advice about someone standing outside your home or breaking into your house physically, not about electronic surveillance via IOT devices.

However, a quick Google search turns up dozens of apps and devices designed to help someone monitor their target via phones, computers and their cars, all with simple step-by-step instructions. (Reference 4)

"Ultimately you can throw away your phone or your FitBit if you fear its security has been compromised; if the compromised device is your home thermostat, however, or your water heater, your alarm system or even an embedded medical device like an insulin implant, disabling or getting rid of it is much more difficult." (Reference 4).

Law enforcement, IOT and family violence

There is often a disconnect between law enforcement and some types of family violence, and we are concerned that using IOT devices to stalk and monitor will make this more pronounced. It will be difficult for a victim to substantiate and explain 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 the behaviour.

Most current options, such as an Apprehended Violence Order, were created to protect the victim from physical contact. They do not protect against monitoring or stalking.

"An Australian study found that police and many community members perceive intimate partner stalking as less serious than stranger stalking (Scott et al.,2010)." (Reference 6).

However, research suggests that those who stalk their partners are particularly persistent and dangerous (Tjaden & Thoennes, 1998, p. 12). (Reference 6).

Intimate partner stalking has been linked to an increased risk of homicide; one study found that 68% of women experienced stalking within the 12 months prior to an attempted or actual homicide (McFarlane, Campbell, & Watson,2002, p. 64). (Reference 6).

Another concern is equipment such as cars being hacked, particularly if the hacker has a history of intimate partner violence.

"In a controlled experiment, two hackers were able compromise a Jeep Cherokee while it was travelling at 70mph by turning the steering wheel and applying the brakes remotely." (Reference 7)

Suggested changes

The following suggested changes are numbered for ease of reference and not in order of priority or magnitude:

1. There needs to be regulation and accountability by manufacturers about the security of internet enabled devices.
2. There should not be a default login encoded into devices.
3. There must be an automated way for security updates to be installed on devices.
4. There must be a simple way for the owner to check who has accessed the device.
5. There should be consumer education on how to protect privacy
6. There should be free access to a helpdesk to take devices to or to consult if a person suspects their device has been compromised.
7. There needs to be Police education on this issue and how to best respond, particularly in family violence situations.
8. Connected vehicles should have advanced technologies like secure boot to ensure the integrity of the vehicle is intact. They should be rebooted every service.
9. There should be extensive and ongoing technology training for anti-domestic violence practitioners about how to respond to and prevent technologically facilitated violence.
10. 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.

References

1. About family violence – Domestic Violence Victoria. (n.d.). Retrieved January 23, 2018, from http://dvvic.org.au/understand/about-family-violence/

2. Violence against women: Additional analysis of the Australian Bureau of Statistics' Personal Safety Survey, 2012. Retrieved January 21, 2018, from http://media.aomx.com/anrows.org.au/PSS_2016update.pdf

3. Al-Alosi, H. (2017, March 27). Technology-facilitated abuse: the new breed of domestic violence. Retrieved January 21, 2018, from http://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683

4. Thomas, E. (2015, November 18). Why the Internet of Things Matters in the Fight Against Domestic Violence. Retrieved January 21, 2018, from https://medium.com/future-crunch/why-the-internet-of-things-matters-in-the-fight-against-domestic-violence-5abc01fed2c2

5. Jones, R. (2017, October 6). Woman's Webcam Starts Following Her Movements And Taunts "Hello." Retrieved January 21, 2018, from https://www.gizmodo.com.au/2017/10/womans-webcam-starts-following-her-movements-and-taunts-hello/

6. Woodlock, D (2015) The Abuse of Technology in Domestic Violence and Stalking | SmartSafe. (n.d.). Retrieved January 21, 2018, from http://www.smartsafe.org.au/abuse-technology-domestic-violence-and-stalking

7. Fearn, N. (2017, February 12). The internet of things can be hacked – and the risks are growing every day. Retrieved January 21, 2018, from http://www.techradar.com/news/the-internet-of-things-can-be-hacked-and-that-puts-your-life-at-risk

End of document