How do we define tech-facilitated abuse?

How does it play out in the context of DFV?

A form of controlling behavior that involves the use of technology to coerce, monitor and <u>maintain</u> surveillance, stalk or harass, threaten, shame and manipulate a current or former intimate partner, and/or children.

GPS Tracking Devices	Air Tags and Blue Tooth devices
• Size ranges from match box sized devices to small box size	• Used from pet tracking to keys, wallet and bag tracking
• Live signal passed from device via SIM card to application or desktop software	• Connected devices share location through encrypted network
• Battery lasts from weeks to months dependant on the type/quality	• Battery life 1 year to 3 years
	• Device safety features to tracking

Nation-wide survey of frontline DFV practitioners, identified a 245% increase between 2015 and 2020 in DFV victims being tracked with GPS apps or devices.

"Woodlock, D., Bentley, K., Schulze, D., Mahoney, N., Chung, D., and Pracilio, A., (2020). Second National Survey of Technology Abuse and Domestic Violence in Australia. WESNET"
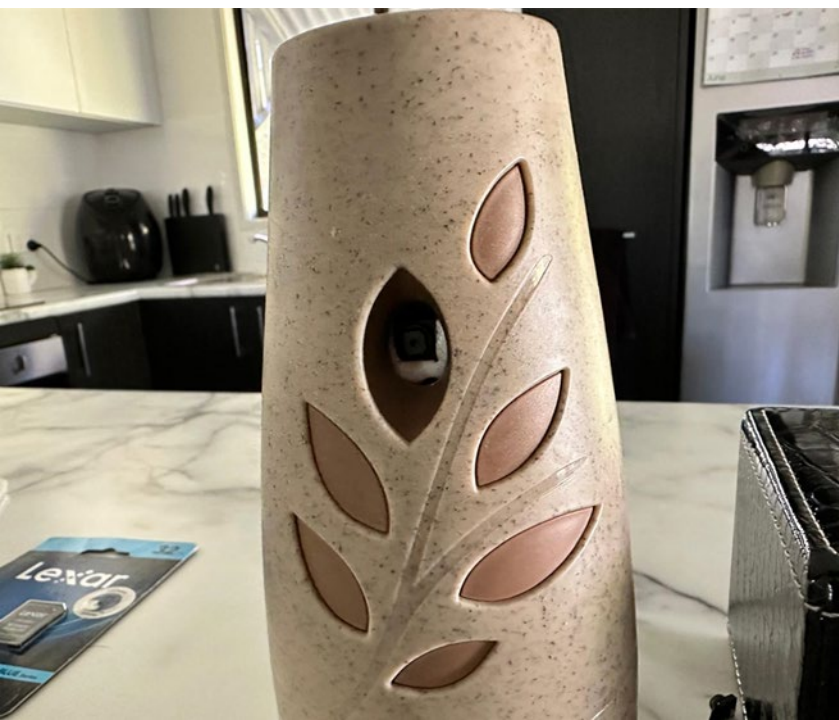
Snapshot: NSW Tracker purchases reviewed

5663 trackers identified

4176 transactions reviewed

3147 customers assessed

Of assessed customers:

- **37%** were adversely known to police
- **25%** had a domestic and family violence background
- **15%** had a serious and organised crime background
- **6%** had a different criminal background
- **126** were AVO defendants at the time of purchase

16%

9%

6%

6%

63%
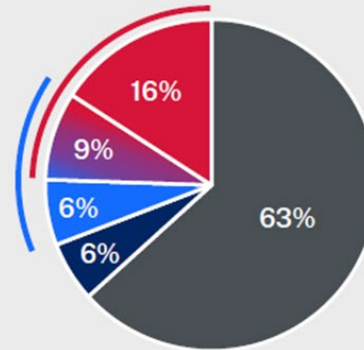
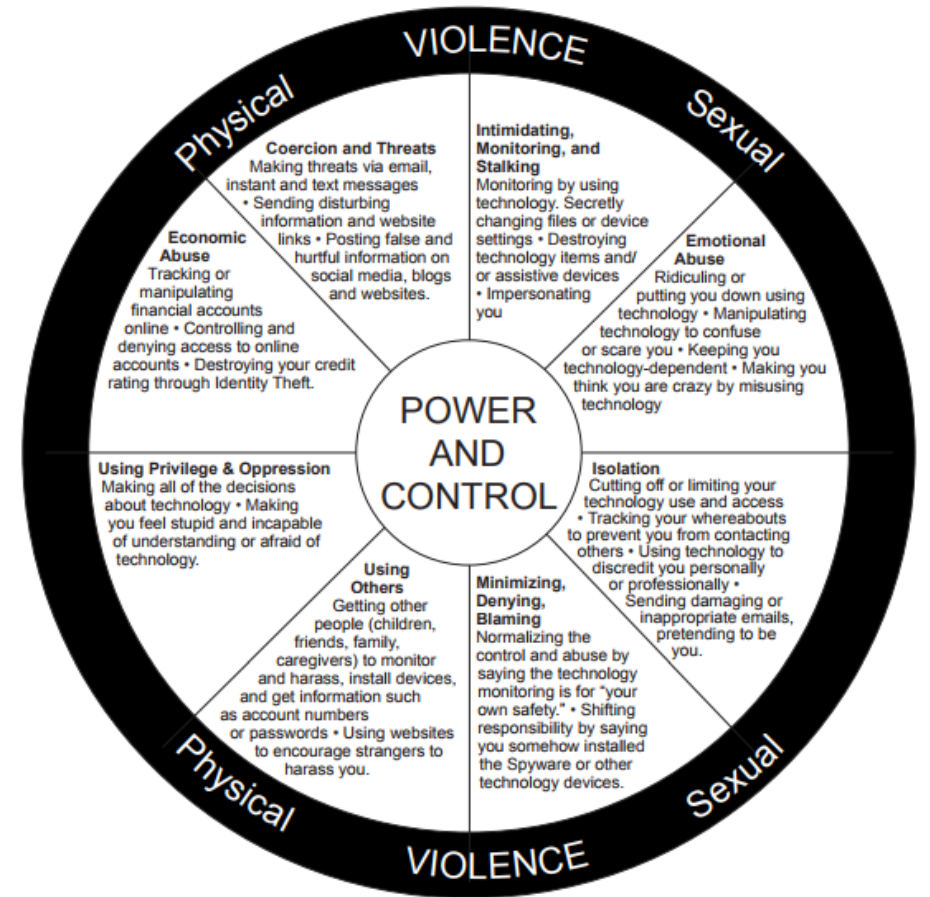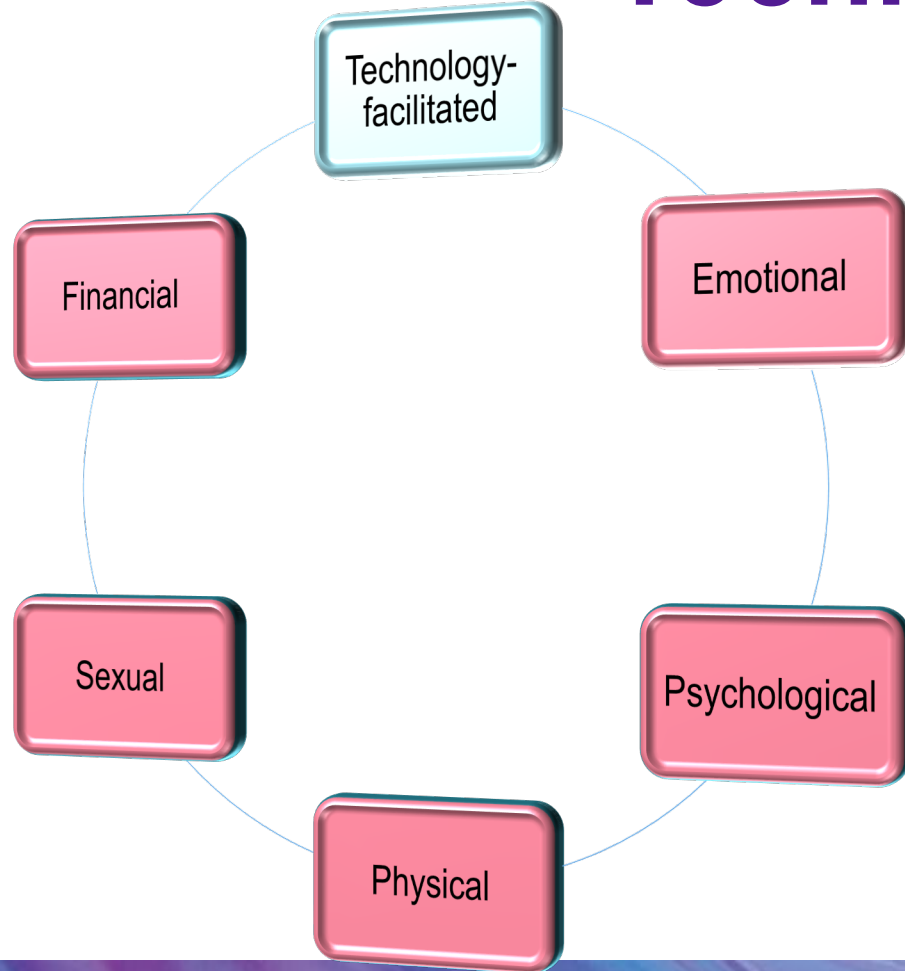**391** high-risk customers referred to police

Intelligence reports or warnings established for all referrals
Some customers remain under investigation

The top 100 customers who purchased the most devices were:

2x more likely to be AVO defendants or charged with domestic and family violence

2.4x more likely to be known for serious and organised crime offending

Technology and DFV

Technology-facilitated

Emotional

Psychological

Physical

Sexual

Financial

Power and Control Wheel

VIOLENCE — Physical · Sexual

Coercion and Threats
Making threats via email, instant and text messages • Sending disturbing information and website links • Posting false and hurtful information on social media, blogs and websites.

Intimidating, Monitoring, and Stalking
Monitoring by using technology. Secretly changing files or device settings • Destroying technology items and/or assistive devices • Impersonating you

Economic Abuse
Tracking or manipulating financial accounts online • Controlling and denying access to online accounts • Destroying your credit rating through Identity Theft.

Emotional Abuse
Ridiculing or putting you down using technology • Manipulating technology to confuse or scare you • Keeping you technology-dependent • Making you think you are crazy by misusing technology

POWER AND CONTROL

Using Privilege & Oppression
Making all of the decisions about technology • Making you feel stupid and incapable of understanding or afraid of technology.

Isolation
Cutting off or limiting your technology use and access • Tracking your whereabouts to prevent you from contacting others • Using technology to discredit you personally or professionally • Sending damaging or inappropriate emails, pretending to be you.

Using Others
Getting other people (children, friends, family, caregivers) to monitor and harass, install devices, and get information such as account numbers or passwords • Using websites to encourage strangers to harass you.

Minimizing, Denying, Blaming
Normalizing the control and abuse by saying the technology monitoring is for "your own safety." • Shifting responsibility by saying you somehow installed the Spyware or other technology devices.

VIOLENCE — Physical · Sexual

http://wesnet.org.au/safetynet/safetynetdocs/

Pros and cons to definitions?

Benefits to defining / categorising

- Aid identification and training
- Enhance prevention efforts
- Locating different tools to be used

This is an evolving field

Definitions are not absolute OR unchanging

Common forms

Use of technology to **enact other forms of abuse and 'traditional' stalking**

Stalking

The **sending or posting of abusive acts or communications** using technology intended to harass or defame

Causing **an unauthorised function or impairing an authorised function** on a device owned by a victim/survivor

Access or denial of access to technologies / **destroying technology**

IB(S)A

Doxing

Impersonation

TFSV and unpacking consent

- **Common in DFV**

- **Trends in pornography and increases in pornography** (e.g. WESNET 2020 study)

- **IBSA** (production, distribution, threats to) **and the increase in deepfakes**

- **Continuum of coercion** (Kelly 1987; Munro, 2010); move beyond the 'real-rape stereotype' by encompassing range of behaviours that **remove an individual's ability to control intimate contact**

- **In the context of coercive control: physical violence is not 'required' to 'obtain' sex**

- **Survival techniques** *and 'survival consent' (Pearce, 2013)*

"...in turn that was pretty hard and something I'm actually still going through the process of deciphering. He just thought he had the rights and really I was a hostage"

Claire (pseudonym)

"I felt that he pushed me to do things that I normally wouldn't have done or wanted to do... It was a little bit degrading, and I did really get upset about it at the start. I wanted to go over there and delete it. And in the end, I've just come to terms with it. It is what it is, he's got what he's got." Shelly (pseudonym)

"my ex also used his phone and (another device) to photograph and record close up images of us having sex. Although I told him on each occasion this made me feel uncomfortable, I felt coerced into complying..."

Fiona (pseudonym)

"[he would] suddenly take photos of me either during or after sex, and I just froze, because I thought, 'what the hell?' But because of the nature of the DV in the relationship, I was actually too scared to simply say to him, 'what are you doing? Please delete that'. I was just, I didn't have rights, I wasn't allowed to say no to him. I wasn't allowed to question him" Mandy (pseudonym)

Children and TFDV

A 'channel' to stalk and gain intel
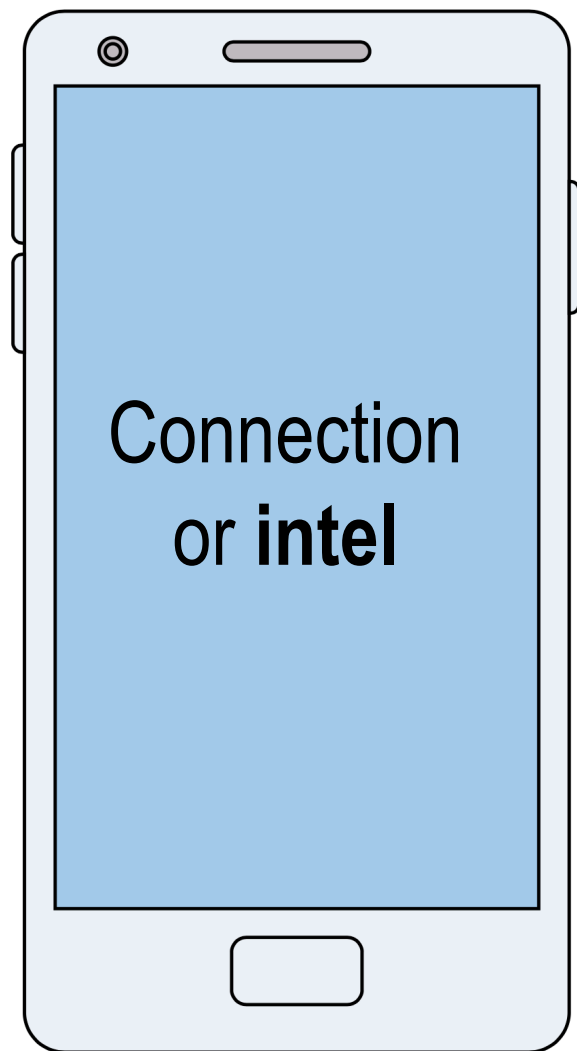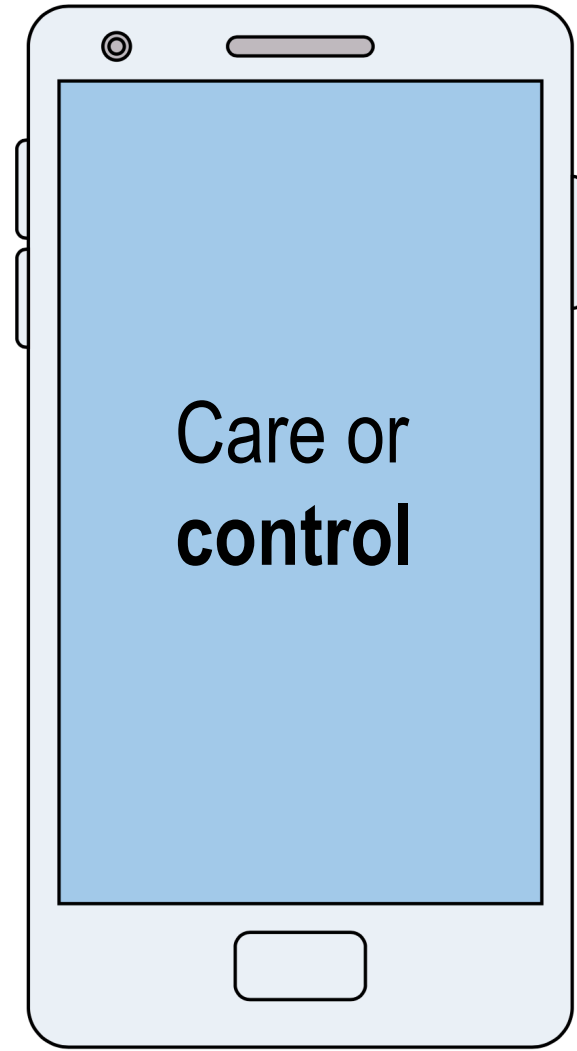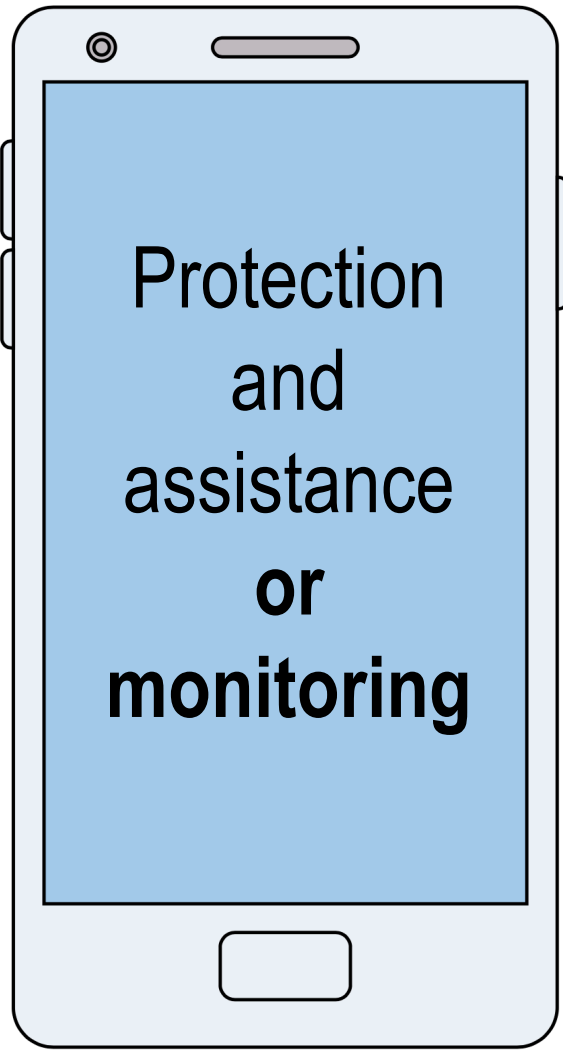
Commissioning children

Contact with children

Controlling children

(Digital) Coercive control

The use of devices and digital media to stalk, harass, threaten and abuse partners, children, third parties

Method (digital), Intent (coercive behaviour) and Impact (control)

Range of (routinely used) techniques, strategies, channels

Patterns of behaviour *individualised*

Tactics / behaviour not typically regraded as 'serious'

Protection and assistance **or monitoring**

Care or **control**

Connection or **intel**

Contact or **attack**

Context (normal, benign *outside*) and individualised 13

What are the impacts on victim-survivor wellbeing and safety?

What risks are associated with TFDV?

Impacts on Wellbeing

- Mental Health challenges- Reality Vs Perception
- Media sensationalising TFA
- Link to women's further reduced confidence
- Women not having control of accounts
- Loans and debt - Digital signatures, Debt etc
- Social Isolation

Impacts on Safety

1 Knowledge in the DV sector

2 Lack of understanding about the impact on women and children

3 Are we moving the women closer to safety or closer to danger

4 Impact of Police response

5 Lack of screening and assessment on TFA and Co Occurring abuse

Impact of Police Response

Rebecca is a single mother who recently separated from her long-term partner after experiencing increased levels of FDV during pregnancy.

Rebecca resides in a two-bedroom apartment and her vehicle is parked in an unsecured carpark in the basement level of the

Rebecca had self-referred after the respondent started turning up at locations she frequented.

Through screening established the respondent would turn up to locations Rebecca had never previously attended.

The respondent would frequently arrive 10-15 minutes after Rebecca would arrive at her location, with particular attention focussed on any restaurant or caffe Rebecca would meet friends.

The respondent would be observed checking on who Rebecca was with prior to leaving.

Rebecca further stated that the respondent would call her if she deviated from her normal day care to home route to question what she was doing.

Impact of Police Response

Technical Surveillance Countermeasure Sweep (TSCM) of her vehicle was conducted and a hidden tracking device was located

Whilst conducting a physical inspection of the device in place, it was established that the device had a anti tamper switch-if removed, would notify the respondent that the device had been tampered with which could result in loss of evidence.

The technician remained with Rebecca to assist with communication with Police

Police from Criminal Investigation Branch (CIB) and Scenes of crime (SOC) attended and captured pictures of the device in place.

CC team were able to explain that the device and reasons why the device should remain in place prior to any search warrant was obtained

CC team closely with Police around the information required to complete the warrant whilst working with Rebecca to ensure a robust safety plan was in place while the device remained on her vehicle.

Outcome:

Police conducted a search warrant at the respondents address where they recovered packaging, software and other related material

Police DVO was applied for and granted

Criminal Code charges currently before the courts

18

Impact of Police Response

The client was a 21-year-old female who had recently separated from her short-term boyfriend and flat mate.

She experienced significant sexual violence, monitoring and coercive control which began early in the relationship.

The client was referred to the Technology Abuse Detection and Assessment Hub by a local Domestic and Family Violence support service.

Upon leaving the relationship, Joan started to receive pizza deliveries to her vehicle within a short time after parking her vehicle

It was identified that the behaviour increased when Joan was in her personal time as opposed to working with her clients

At the time of Joan attending the tech hub, a Dominos pizza delivery bike was observed on the adjoining road.

At this time, Joans vehicle was placed on our hoist and a scan and inspection was conducted where a tracking device was located.

At this time, QPS Scenes of Crime (SOC) attended and captured evidence of the tracking device located in situ on the vehicle.

Police then removed the device and lodged as evidence.

Outcome:

Extensive safety planning had to be put in place as the respondent had lost the ability to monitor Joan electronically increasing the risk of physical surveillance

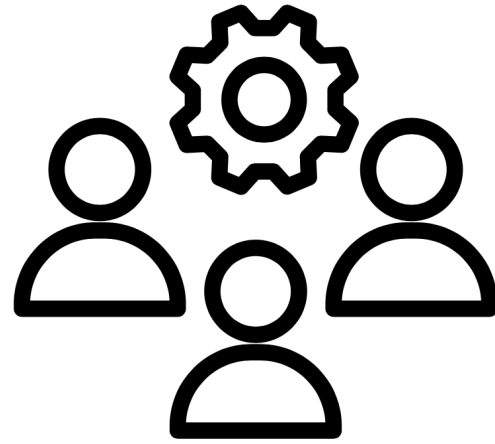4 x recent breaches a result of physical surveillance

Further safety upgrades were carried out to deter the respondent and capture further evidence of ongoing surveillance
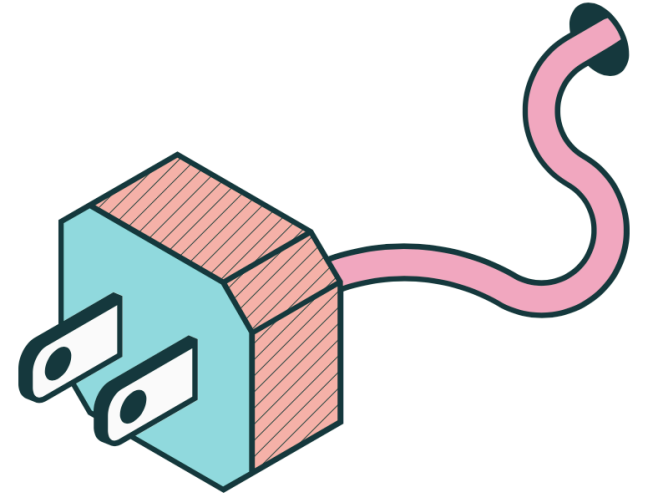
19
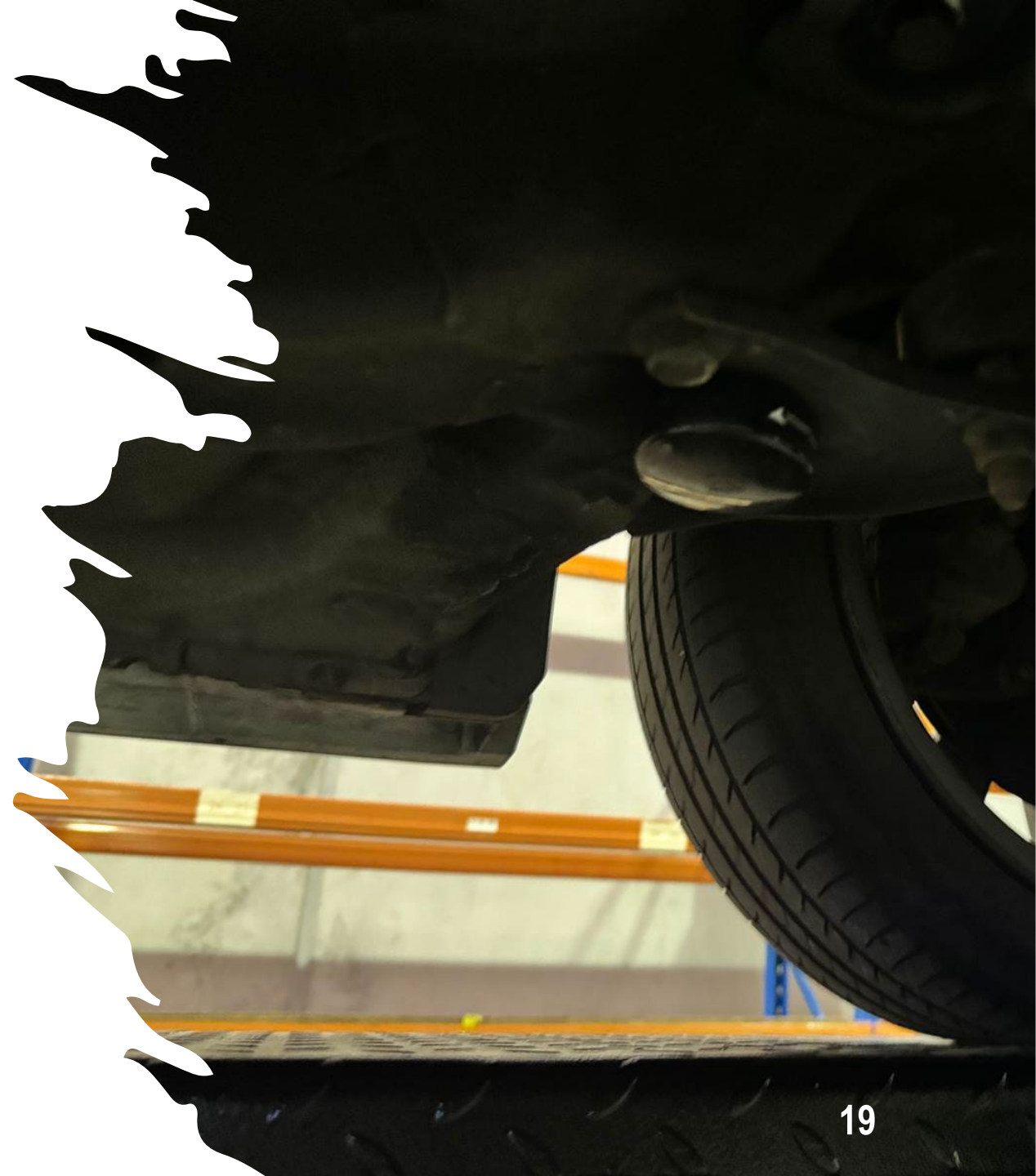
Intimate Threat Model

Domestic setting   **Relational dynamics**   **Power**

Impacts

Technology becomes a **weapon**

Threatens **freedom, rights, engagement**

Trauma triggers

Health and **wellbeing**

Feeling **'crazy'** and **'paranoid'**

Fear and **sense of security**

Inescapable

Powerlessness

Self-harm

'Safety work'

Intel: homicide flags and risk

Obsessive behaviours

Death threats

Monitoring and stalking

Non-fatal strangulation

NOTE: risks associated with disengagement

Separation

- **Perpetrators and control:** during separation TFV typically begins or escalates

- *Separation assault* is **related to the severity and frequency of abuse prior to separation**

- **Post separation** is a key context for TFV

7%

93%

■ No abuse ■ Abuse
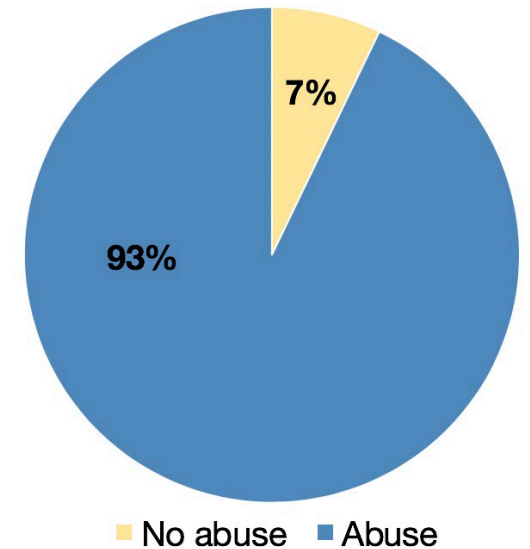
Intersectionality: context, impact and risk

First Nations victim-survivors

Migrant and refugee victim-survivors

LGBTQIA+

Cognitive, intellectual, physical disability

RRR

How can we respond to and prevent this harm?

Can we harness technology to address DFV?

71%	70%	68%	61%	41%
Stalking	Emotional	Sexual	Financial	Physical
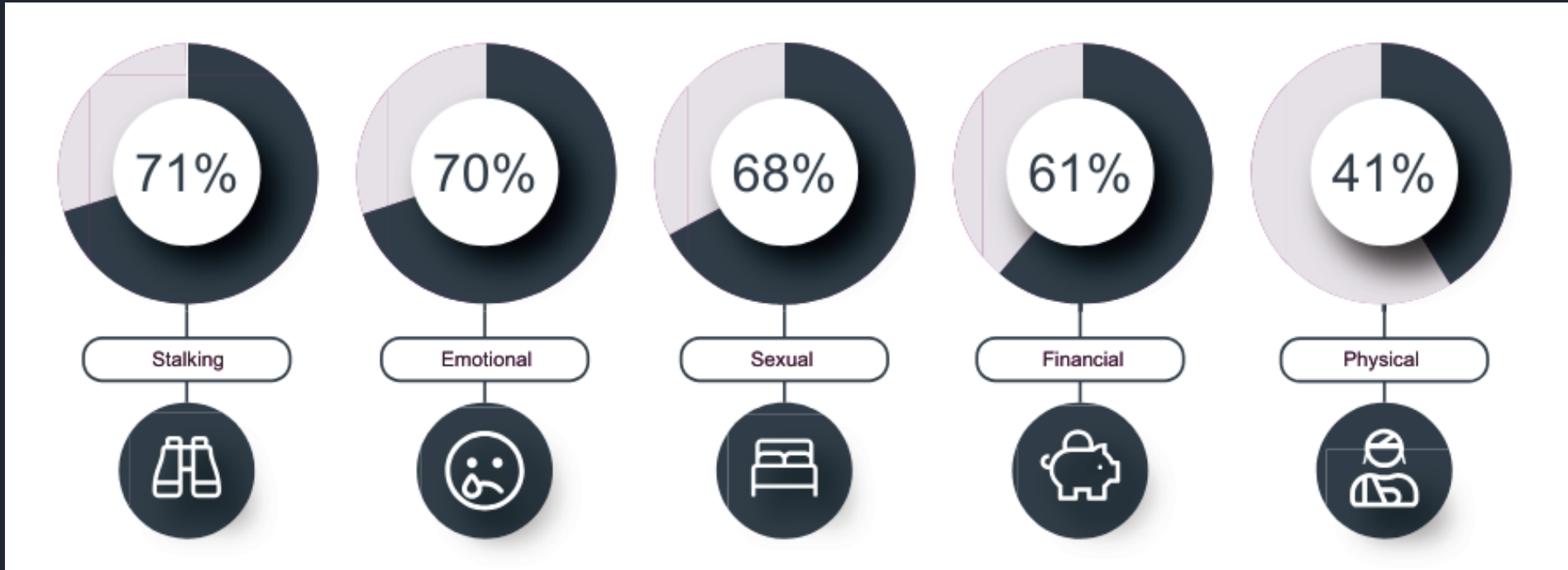
- Utilise experience outside the sector Safety Planning, methods to disrupt TFA and the link with safety upgrade programs from an holistic approach

- Further operational training for Police and organisations – What's on the ground

- Safety planning around technology and understanding the Co Occurring forms of Violence and how they are identified and linked

- Increase operational Programs - Almost all survey respondents (99.3%) stated that they had clients who had experienced technology facilitated abuse

Survivor **suspicions and instinct**

Validation

Safety planning / work

What has been **documented / reported** and to who?

Risks

Seeking intel and investigating

Discussions about discomfort, unease, displeasure: *behaviours that made you uneasy, uncomfortable*

Context and the notion of consent: *recognising lived reality of coercive control*

Considering **normalisation and shifting norms**

Recognising perpetrator intent: *recognising settings, dynamics, concerns*

Trauma-informed and acknowledging impact: *across domains of victim-survivor lives and support*

Digital coercive control toolkit

Holistic view	Position as DCC	Intimate Threat Model	Overt / covert
Access	Risk including separation	Tech-capabilities	Validation

Abusive behaviours and negative emotions

Anger

Fear

Suspicion

Sadness

Inhibitors of abusive behaviour

FOSTERING ALTERNATIVE
RESPONSES
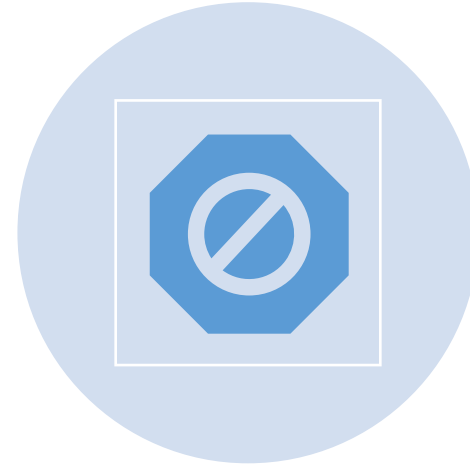
OPPORTUNITIES FOR
INTERRUPTION OR INTERVENTION

Capacity building, enhancing responses

Capturing perpetrator narratives, strategies, manipulation

-Because I have been very nice to you...Very patient...

-I see myself in a mirror and it seems as if I have the body of a woman

Police; _almost always for 'crisis' training_

Courts; _'visualising crime scenes' and to 'bring the victim into the courtroom'_
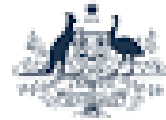
Probation; _facilitating rehabilitation_
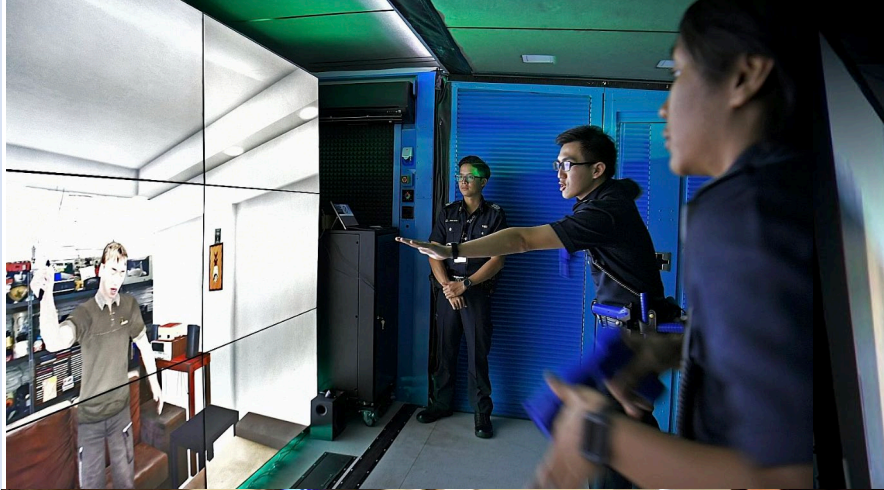
Keeping perpetrators in focus

Bridget.Harris@monash.edu

gkillen@concentricconcepts.com.au