COMPUTER SCIENCE

GENDER AND TECHNOLOGY

UCL

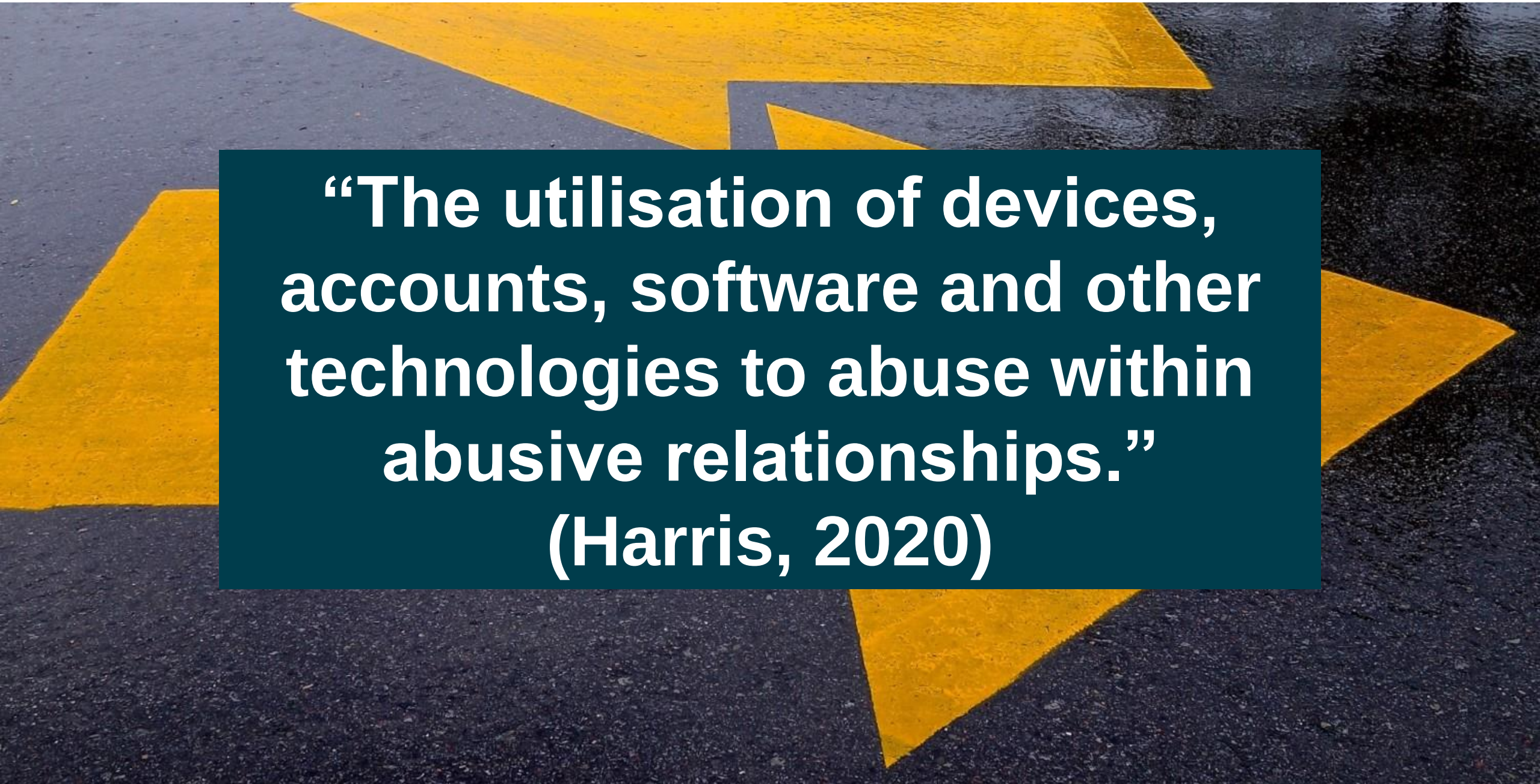
Tech Abuse and Practitioner Guidance

The Implications of technology-facilitated abuse on Victims/Survivors including those with Disabilities, of Gender-Based Domestic Violence & Abuse

Demelza Luna Reaver

What?
Why?
How?

What?


“The utilisation of devices, accounts, software and other technologies to abuse within abusive relationships.”
(Harris, 2020)

Text Messaging
Stalkerware
Trackers
Impersonation
Image-Based Abuse

Misuse/repurposing

“Conventional” technologies

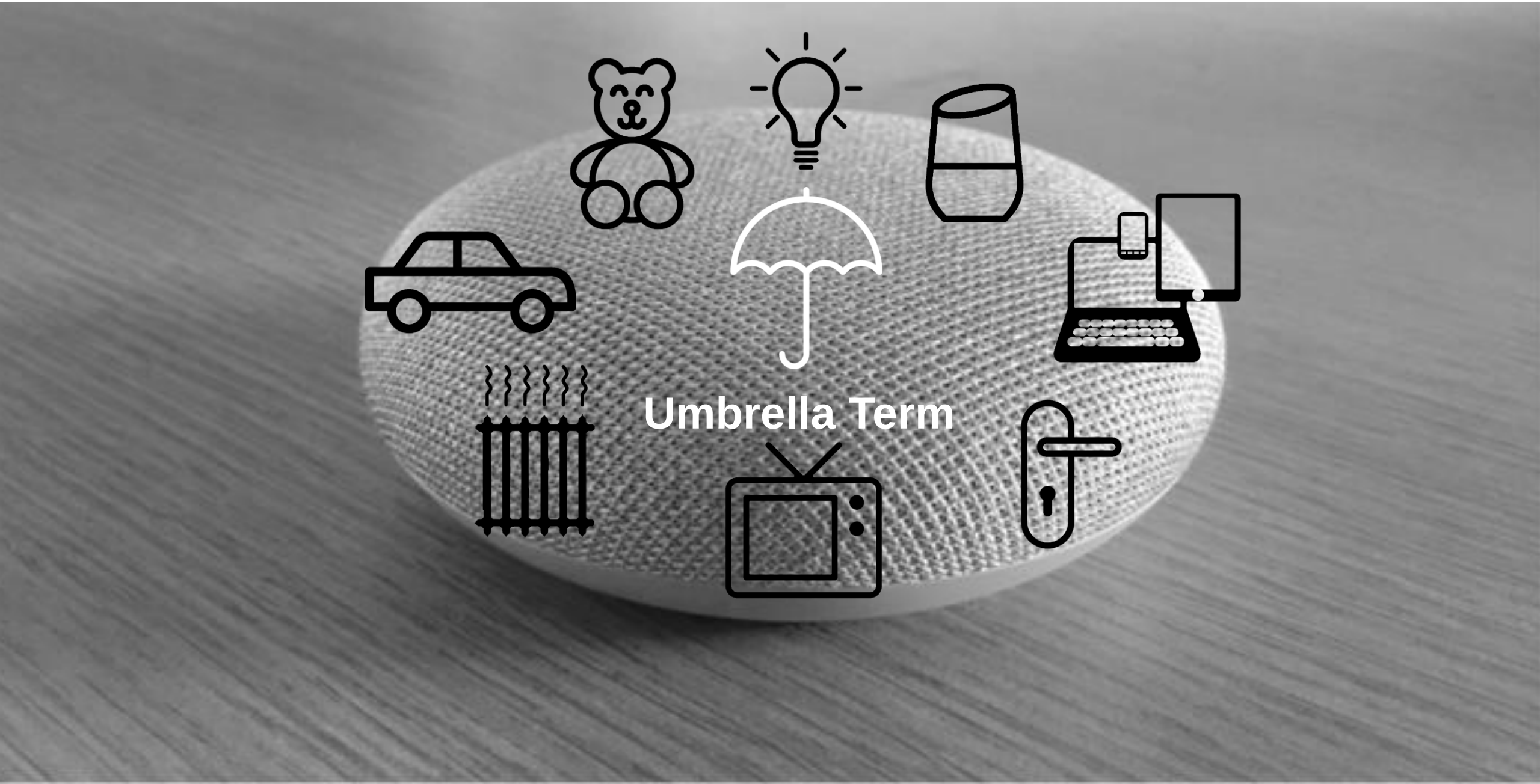
Women and BAME

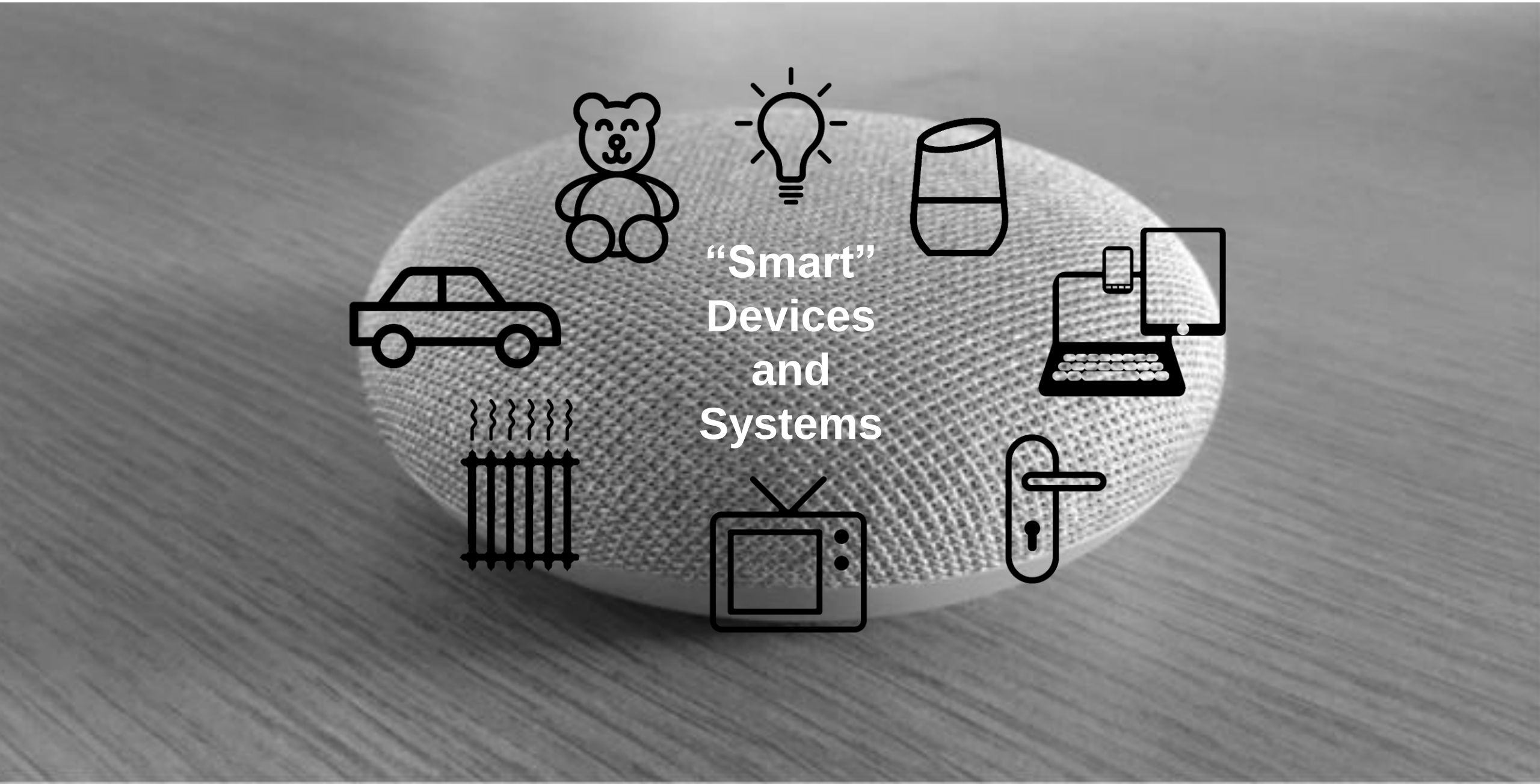
“Active” commitment

Predefined ideas

Technology is changing

Internet of Things


Umbrella Term


“Smart” Devices and Systems

Risks

Uncertainty

Opportunities

Voice control

Video recording

Shared accounts

Remote control

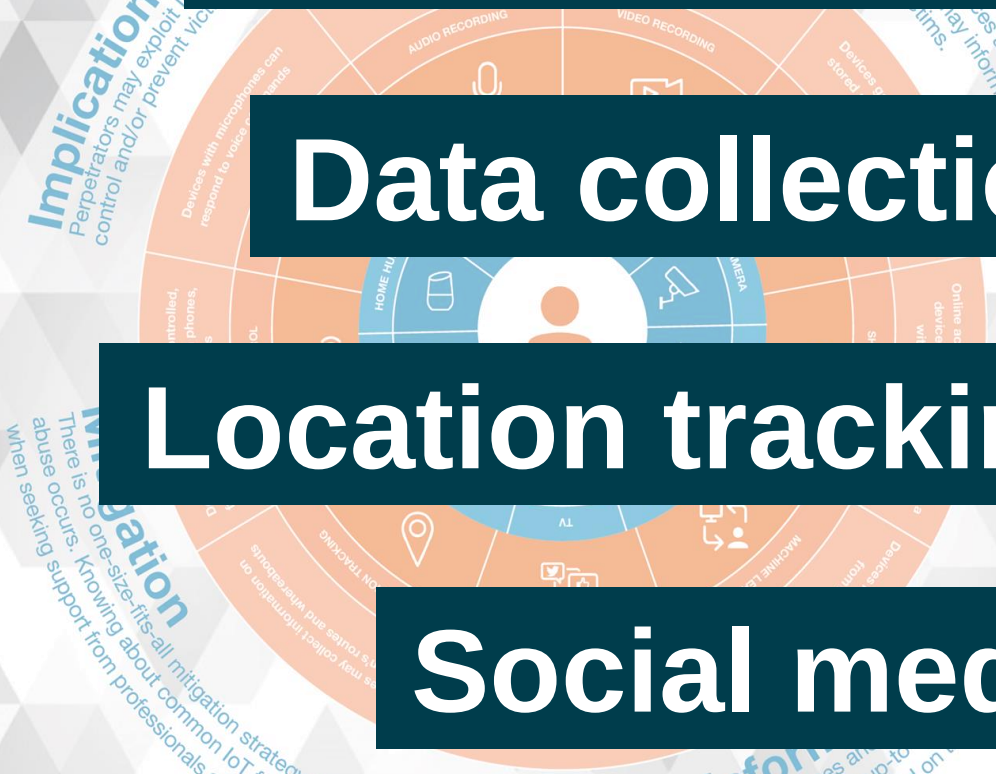
Machine learning

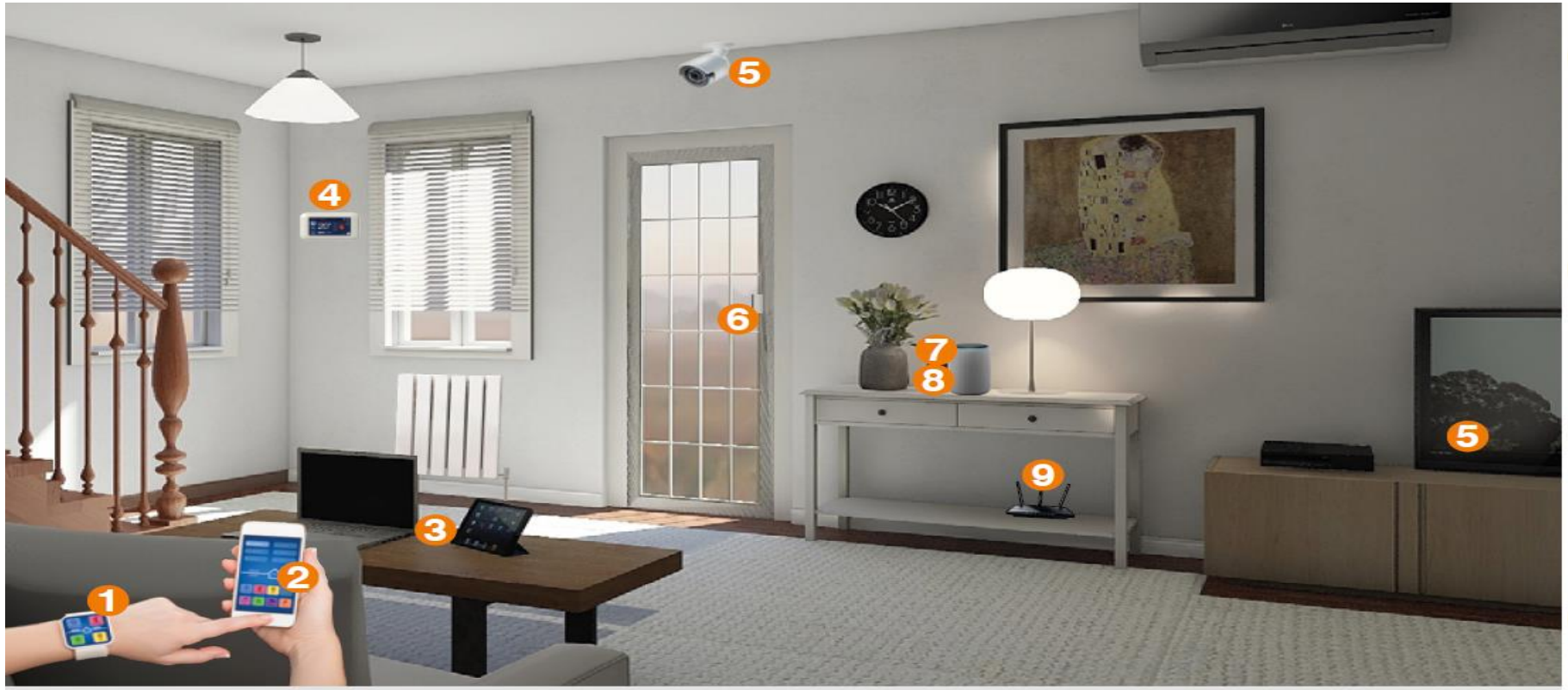
Audio recording

Data collection

Location tracking

Social media





Tech Abuse — Smart, Internet-connected devices present new risks for victims of domestic violence & abuse

1 Wearable devices
Could allow perpetrators to track and monitor movements and other behavioural patterns drawing on GPS signals and other collected data.

2 Phones
Could provide perpetrator an access point to control various IoT devices.

3 Laptops and tablets
Accounts between devices are linked and could allow perpetrators to change and review IoT devices' settings via an Internet browser.

4 Remote control of heating, lighting and blinds
Could be used to coerce and intimidate victims by switching systems on or off from afar.

5 Security cameras and TVs
Could facilitate remote monitoring and online stalking; video recording could facilitate image-based abuse (such as revenge porn).

6 Smart security
Could provide access to doors through voice activation, apps, or electronic key codes.

7 Audio recording
Could facilitate remote monitoring and stalking.

8 Voice control
May enable perpetrators to contact the victim as well as trace and review a person's history of commands and purchases.

9 Router
Connects all smart home devices to the Internet.

Why?

Negative
Positive

Precautionary Behaviors

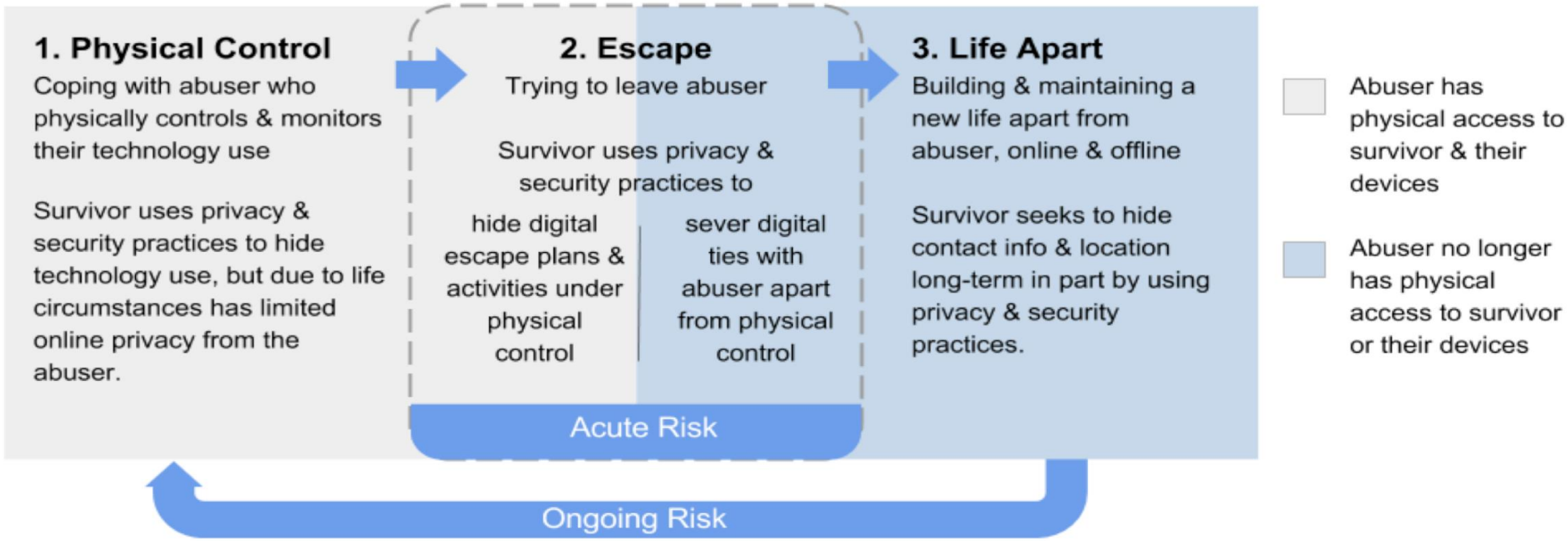


Figure 1. Three phases of IPA that affected technology use, focusing on privacy & security practices.

Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shelton, M., … Consolvo, S. (2017). Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 2189–2201. New York, NY, USA: ACM. https://doi.org/10.1145/3025453.3025875

Design ≠ “Security in Mind”

Intimate Partner Threat Model

Disguised

Enhanced functionalities

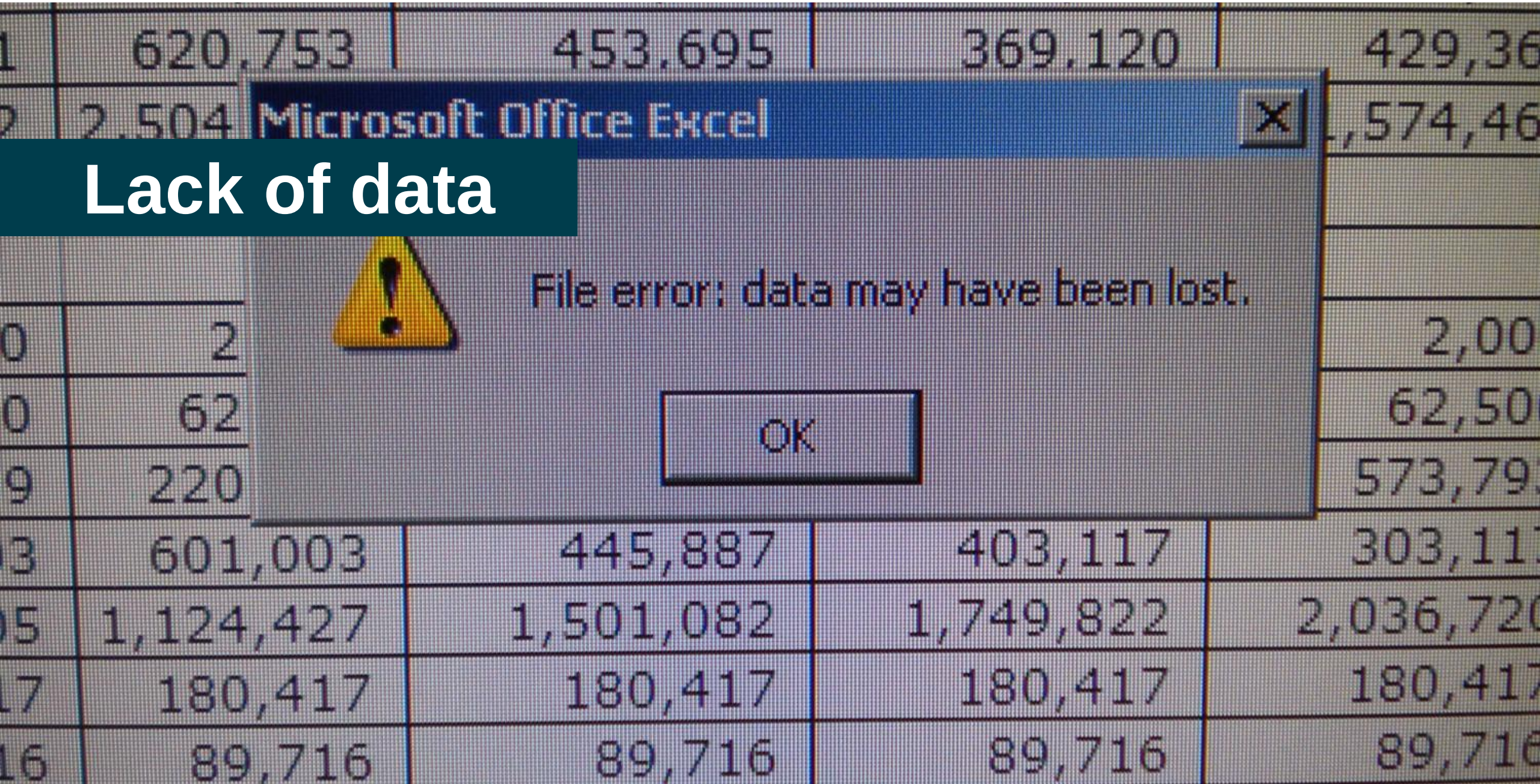
Expanding and exacerbating reach

Underestimation

Overestimation

Support Sector: Overload

Lack of data


Microsoft Office Excel
File error: data may have been lost.
OK

97% of Australian case workers said stated that perpetrators were using technology to stalk victims (SmartSafe, 2014)

72% of Refuge (2020) service users identify experiencing tech abuse

85% of respondents received online abuse from a partner or ex-partner (Women's Aid, 2018)

How?

National Statistics

National Statistics

British Crime Survey: methodology

Explanation of how the British Crime Survey is conducted, and which areas of the UK it covers.

Published 19 January 2012
From: Home Office

Ending domestic abuse

SafeLives Dash risk checklist
Quick start guidance

You may be looking at this checklist because you are working in a professional capacity with a victim of domestic abuse. These notes are to help you understand the significance of the questions on the checklist. Domestic abuse can take many forms but it is usually perpetrated by men towards women in an intimate relationship such as boyfriend/girlfriend, husband/wife. This checklist can also be used for lesbian, gay, bisexual relationships and for situations of 'honour'-based violence or family violence. Domestic abuse can include physical, emotional, mental, sexual or financial abuse as well as stalking and harassment. They might be experiencing one or all types of abuse; each situation is unique. It is the combination of behaviours that can be so intimidating. It can occur both during a relationship or after it has ended.

The purpose of the Dash risk checklist is to give a consistent and simple tool for practitioners who work with adult victims of domestic abuse in order to help them identify those who are at high risk of harm and whose cases should be referred to a Marac meeting in order to manage their risk. If you are concerned about risk to a child or children, you should make a referral to ensure that a full assessment of their safety and welfare is made.

The Dash risk checklist should be introduced to the victim within the framework of your agency's:

- Confidentiality policy
- Information sharing policy and protocols
- Marac referral policies and protocols

Before you begin to ask the questions in the Dash risk checklist:

- Establish how much time the victim has to talk to you: is it safe to talk now? What are safe contact details?
- Establish the whereabouts of the perpetrator and children
- Explain why you are asking these questions and how it relates to the Marac

While you are asking the questions in the Dash risk checklist:

- Identify early on who the victim is frightened of – ex-partner/partner/family member
- Use gender neutral terms such as partner/ex-partner. By creating a safe, accessible environment LGBT victims accessing the service will feel able to disclose both domestic abuse and their sexual orientation or gender identity.

Risk Assessment

Safety Plan

TALK TO SOMEONE YOU TRUST

Whether it be a family member, neighbor, colleague, us or a local shelter.

KEEP EVIDENCE OF ABUSE

Screenshots of texts, photos of physical harm, letters, police reports, dates, times and locations.

PACK A SUITCASE OR BAG

Include important documents, passport, ID,

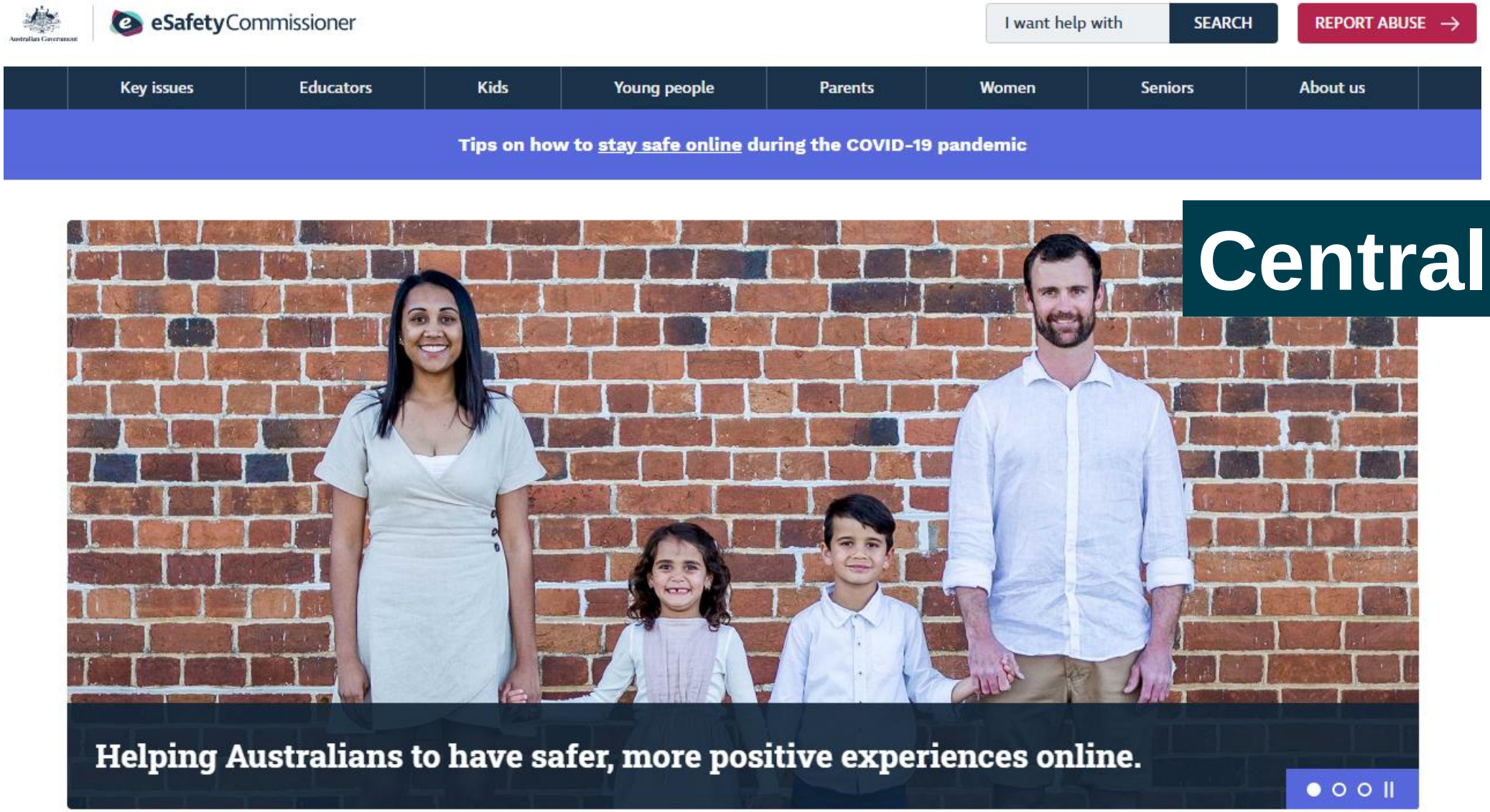
Perpetrator Programmes

US

Australia
OOROO

Align Policy
Cybercrime
Domestic Abuse
Stalking
Harassment

Centralisation



Tech Abuse Clinic

https://www.ceta.tech.cornell.edu/

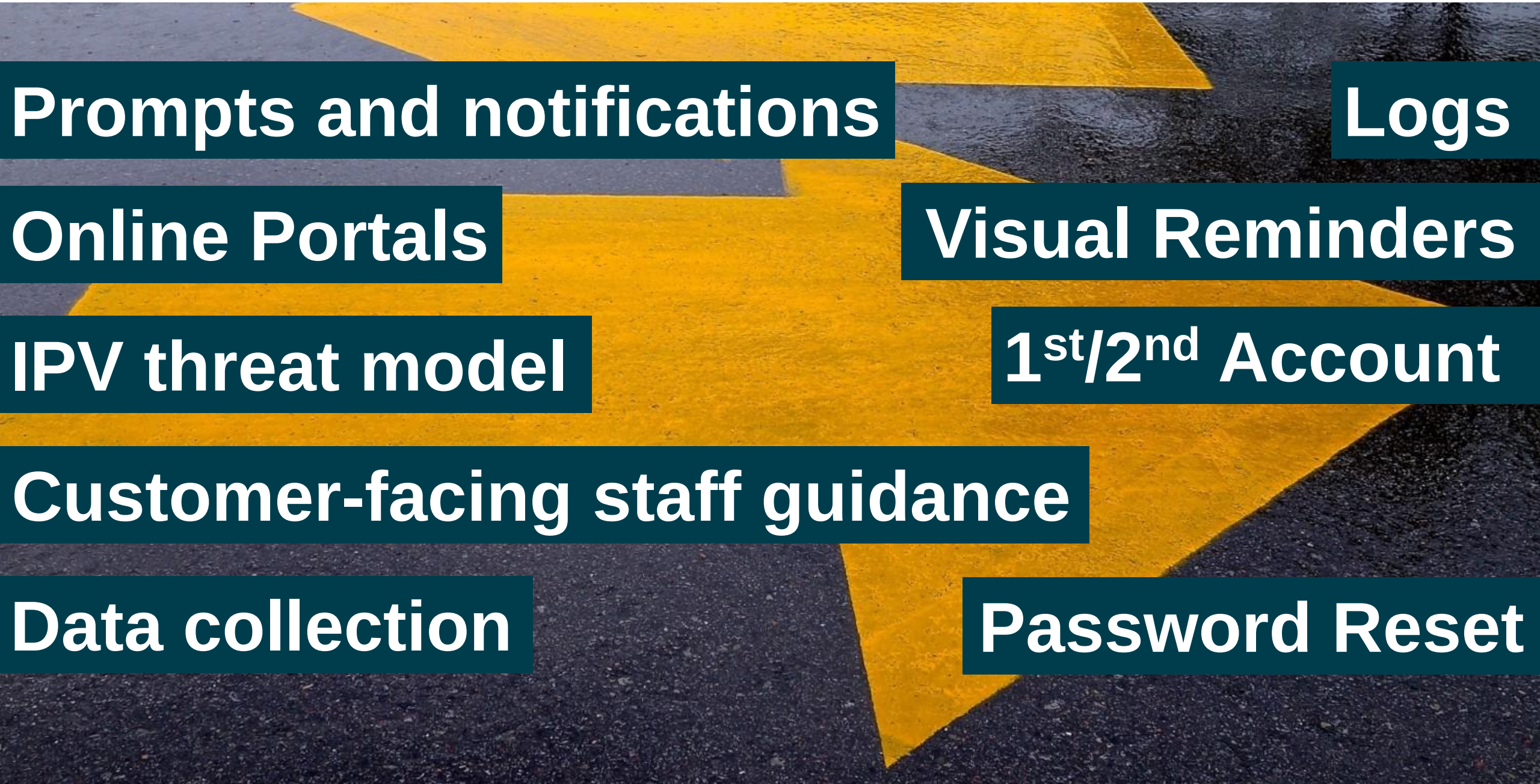
CETA

CLINIC TO END TECH ABUSE

The Cyber Helpline

https://www.thecyberhelpline.com/

Pointers for Industry


Prompts and notifications
Logs
Online Portals
Visual Reminders
IPV threat model
1st/2nd Account
Customer-facing staff guidance
Data collection
Password Reset

Data
Risk Assessment
Pressure Industry
Align Policy
Training/Support
Safety Plan

Further Information

UCL COMPUTER SCIENCE

Home Study Research Collaborate News and events People About

UCL Home » UCL Computer Science » Research » Research groups » Gender and Tech

Gender and Tech
Gender and IoT
RespondXR: Digital vulnerability of immersive training for first responders
Tackling Technology-Facilitated Abuse to Protect Victims and Survivors of Intimate Partner Violence
The UK Computer Misuse Act 1990 and cases of technology-enabled domestic

Gender and Tech

The Gender and Tech Research Group investigates the intersection points of technology, security, and gender to make digital systems work for everyone.

Newsletter

Subscribe to keep up-to-date with our research progress, any latest developments in the space of technology-facilitated abuse and the Internet of Things, as well as training and support opportunities.

Sign up

Contact

Dr Leonie Maria Tanczer
Associate Professor in International Security and Emerging Technologies

UCL Computer Science

Demelza Luna Reaver
Luna.reaver.21@ucl.ac.uk

Thank you.

#GIoT