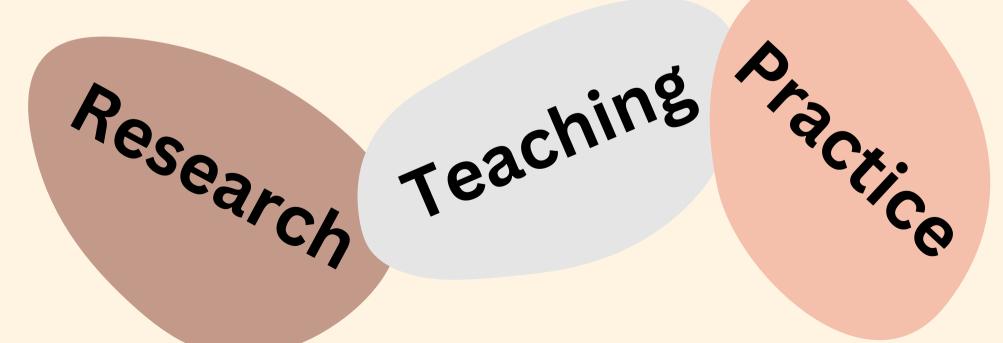


THE ROLE OF IOT IN THE CONTEXT OF INTIMATE PARTNER VIOLENCE

Dr Leonie Maria Tanczer University College London

@leotanczt // @leotanczt@mastodon.social

On the one hand, we study how and why gendered assumptions mould our technological systems and affect their representation, design, as well as usage and control.



Gender & Tech

On the other hand, we examine the dynamics that enable digital technologies to construct and reinforce gender and other social categories such as race, class, age, or sexuality.

TECHNOLOGY IS GENDERED

Phone size

Bicycles

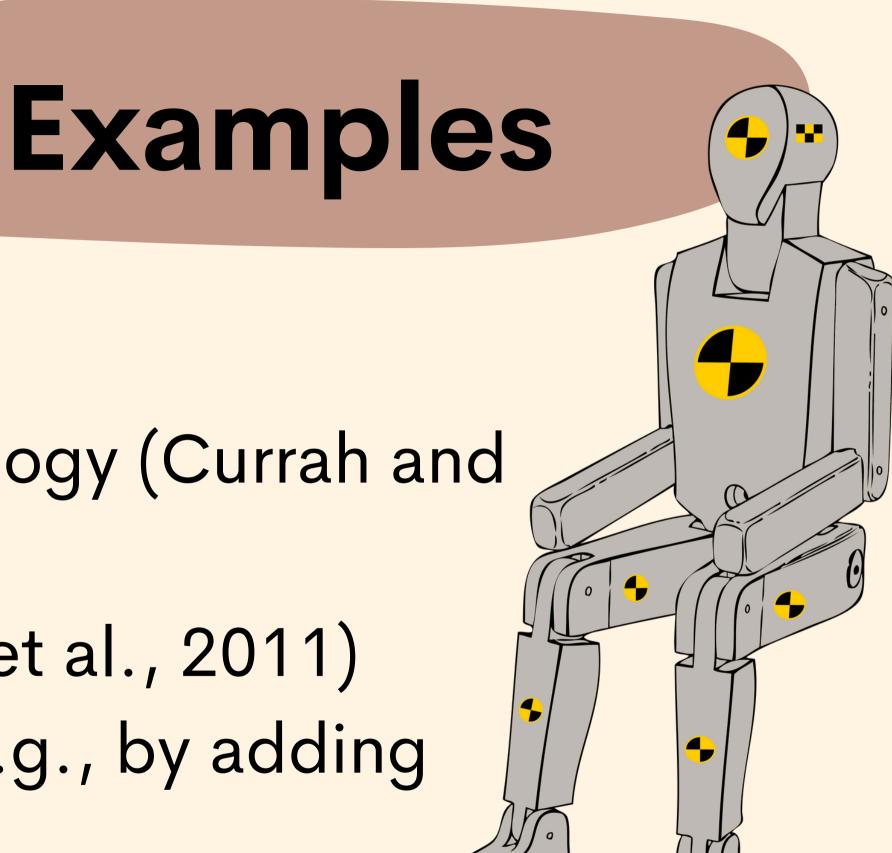
• fMRI scans (Kaiser, 2010)

Advanced Imaging Technology (Currah and

Mulqueen, 2011)

Crash test dummies (Bose et al., 2011)

• "Making things prettier," e.g., by adding different colours, mirrors etc.



Gendered Nature

"women and men have different access to the creation of technology, have different access to decision making about the development of technology, and have different experiences with technology." (Rakow, 1988)

Representation
Design
Usage/Control
Effects









A growing body of work:

- Online harassment
- Cyberstalking
- Spyware
- Image-based abuse

. . .

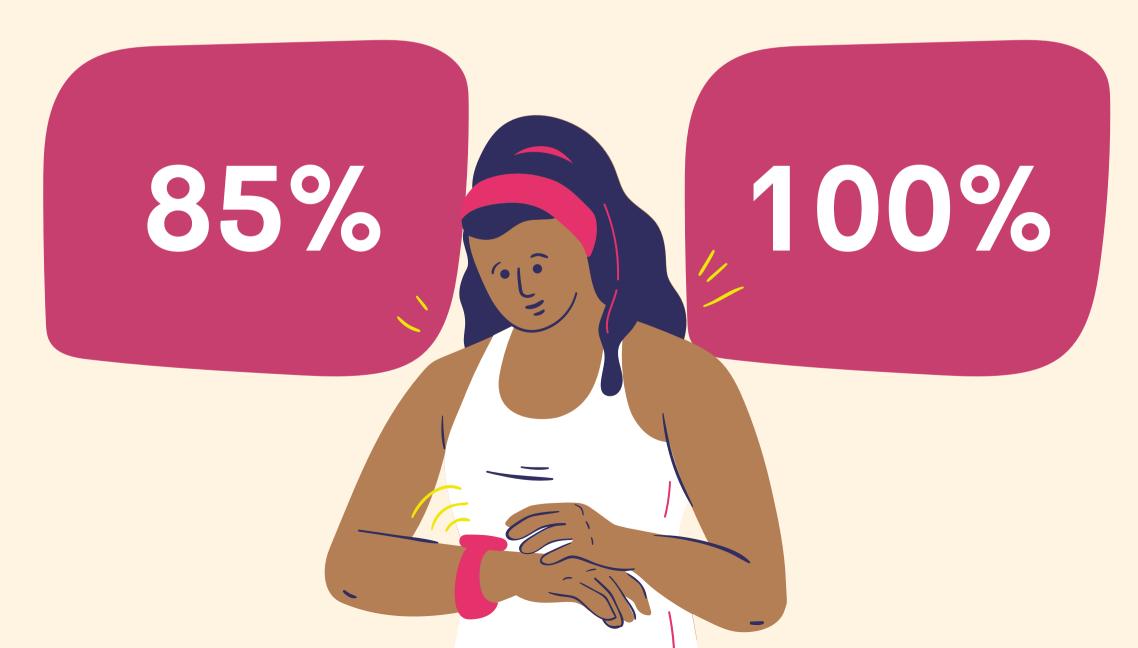
TECH ABUSE

Tech permeates every aspect of our life.

Refuge

Women's Aid Stalking Helpline

72%





Predefined Ideas

- Perpetrator/criminal
- Abuse
- Technologies



TECHNOLOGY IS CHANGING

GENDER AND IOT

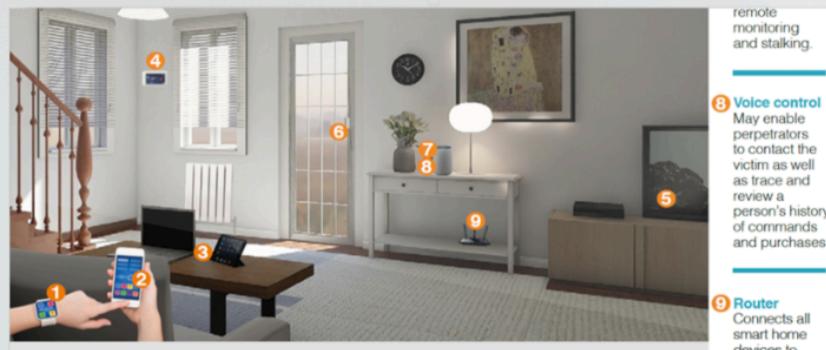
How will the Internet of Things (IoT) impact gender-based domestic violence and abuse, and what socio-technical measures will need to be implemented in order to mitigate against those risks?



"Smart" Abuse?

Increasingly household devices are now "smart, but...

- **Disguised** in terms of their ability to sense, accentuate, and collect private data;
- >>They look like "normal" devices we are used to
- They have new, "enhanced" functionalities
- >> Expanding and exacerbating the reach of coercive and controlling behaviour



Smart, Internet-connected devices present new

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

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

Phones

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

Remote control of heating, lighting and blinds

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

remote monitoring and stalking.

May enable perpetrators to contact the victim as well as trace and review a

person's history of commands and purchases.

Router

Connects all smart home devices to

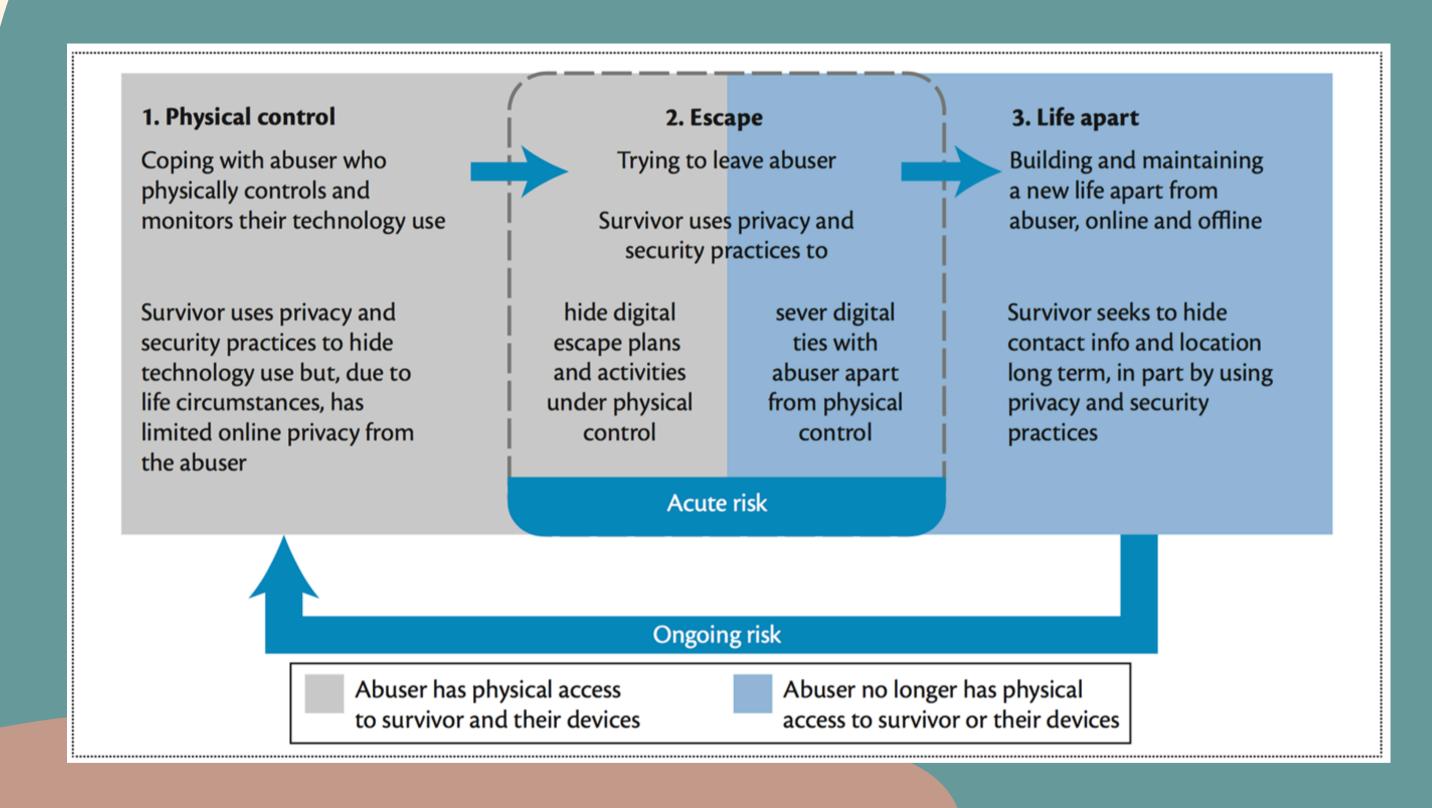
the Internet.

Smart security
 Could provide access to doors



- Voice control
- Audio recording
- Video recording
- Data collection
- Shared accounts
- Location tracking
- Remote control
- Social media
- Machine learning

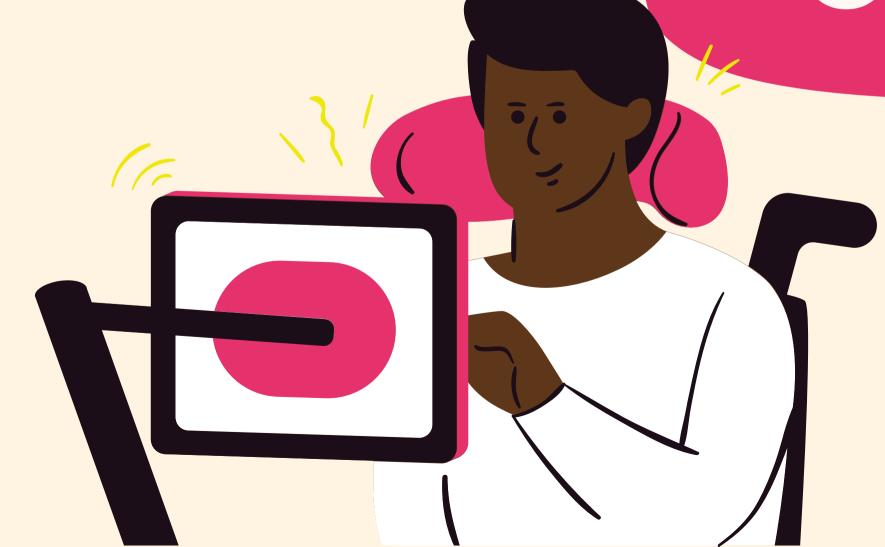
The perpetrator is a "UI-bound adversary"



Risk Trajectories

Underestimation







Support Sector

Tech Industry

Government Policy



Working Group

IEEE - P2987: Recommended Practice for Principles for Design and Operation Addressing TechnologyFacilitated Inter-personal Control

NEWSLETTER



