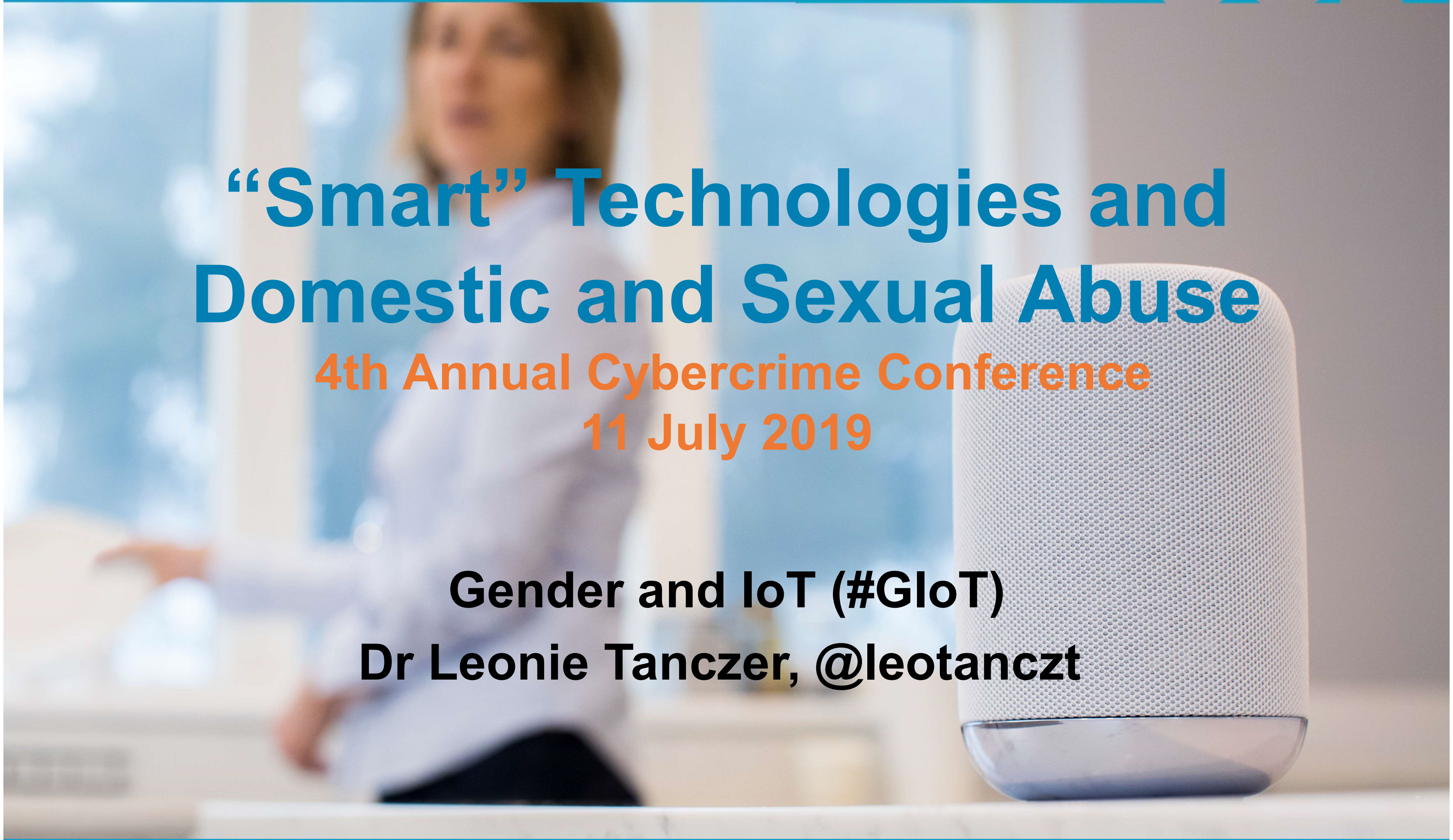
SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY



“Smart” Technologies and Domestic and Sexual Abuse

4th Annual Cybercrime Conference

11 July 2019

Gender and IoT (#GIoT)

Dr Leonie Tanczer, @leotanczt

SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

Technology is gendered.

STE@PP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world

Examples?

- 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 of technology

"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

Technology is abused.

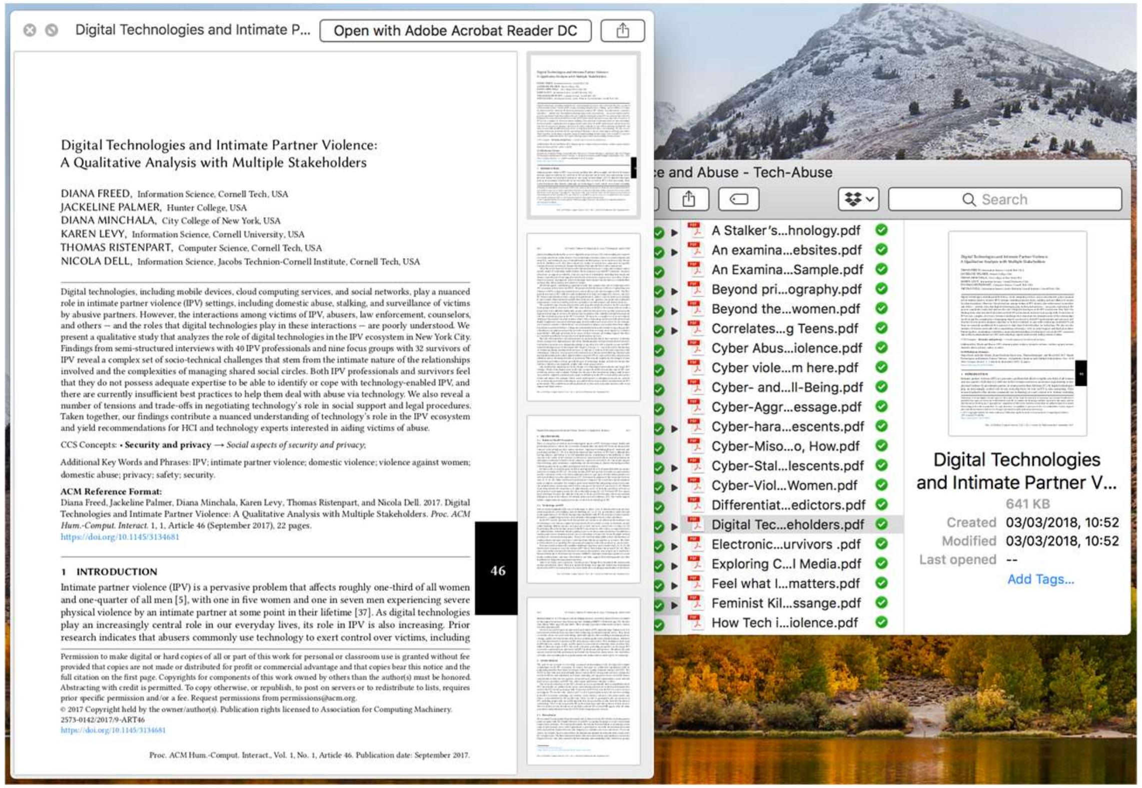
SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

A MAN HAS CREATED A MACHINE. NOW THE MACHINE WANTS TO CREATE A MAN . . .
Demon Seed
AA
MGM presents a HERB JAFFE PRODUCTION JULIE CHRISTIE in "DEMON SEED" co-starring FRITZ WEAVER
Produced by HERB JAFFE Directed by DONALD CAMMELL Screenplay by ROBERT JAFFE, ROGER O. HIRSON
Musical Score Composed and Conducted by JERRY FIELDING Filmed in PANAVISION® and METROCOLOR®
MGM
READ THE CORGI PAPERBACK
Distributed by CINEMA INTERNATIONAL CORPORATION

https://www.vintagemovieposters.co.uk/shop/demon-seed-movie-poster/

Growing body of work…

“Tech Abuse”



Digital Technologies and Intimate P...
Open with Adobe Acrobat Reader DC

Digital Technologies and Intimate Partner Violence:
A Qualitative Analysis with Multiple Stakeholders

DIANA FREED, Information Science, Cornell Tech, USA
JACKELINE PALMER, Hunter College, USA
DIANA MINCHALA, City College of New York, USA
KAREN LEVY, Information Science, Cornell University, USA
THOMAS RISTENPART, Computer Science, Cornell Tech, USA
NICOLA DELL, Information Science, Jacobs Technion-Cornell Institute, Cornell Tech, USA

Digital technologies, including mobile devices, cloud computing services, and social networks, play a nuanced role in intimate partner violence (IPV) settings, including domestic abuse, stalking, and surveillance of victims by abusive partners. However, the interactions among victims of IPV, abusers, law enforcement, counselors, and others – and the roles that digital technologies play in these interactions – are poorly understood. We present a qualitative study that analyzes the role of digital technologies in the IPV ecosystem in New York City. Findings from semi-structured interviews with 40 IPV professionals and nine focus groups with 32 survivors of IPV reveal a complex set of socio-technical challenges that stem from the intimate nature of the relationships involved and the complexities of managing shared social circles. Both IPV professionals and survivors feel that they do not possess adequate expertise to be able to identify or cope with technology-enabled IPV, and there are currently insufficient best practices to help them deal with abuse via technology. We also reveal a number of tensions and trade-offs in negotiating technology's role in social support and legal procedures. Taken together, our findings contribute a nuanced understanding of technology's role in the IPV ecosystem and yield recommendations for HCI and technology experts interested in aiding victims of abuse.

CCS Concepts: • **Security and privacy** → *Social aspects of security and privacy*;

Additional Key Words and Phrases: IPV; intimate partner violence; domestic violence; violence against women; domestic abuse; privacy; safety; security.

ACM Reference Format:
Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proc. ACM Hum.-Comput. Interact.* 1, 1, Article 46 (September 2017), 22 pages.
https://doi.org/10.1145/3134681

46

1 INTRODUCTION

Intimate partner violence (IPV) is a pervasive problem that affects roughly one-third of all women and one-quarter of all men [5], with one in five women and one in seven men experiencing severe physical violence by an intimate partner at some point in their lifetime [37]. As digital technologies play an increasingly central role in our everyday lives, its role in IPV is also increasing. Prior research indicates that abusers commonly use technology to exert control over victims, including

2573-0142/2017/9-ART46
https://doi.org/10.1145/3134681

A Stalker's...hnology.pdf
An examina...ebsites.pdf
An Examina...Sample.pdf
Beyond pri...ography.pdf
Beyond the...women.pdf
Correlates...g Teens.pdf
Cyber Abus...iolence.pdf
Cyber viole...m here.pdf
Cyber- and...ll-Being.pdf
Cyber-Aggr...essage.pdf
Cyber-hara...escents.pdf
Cyber-Miso...o, How.pdf
Cyber-Stal...lescents.pdf
Cyber-Viol...Women.pdf
Differentiat...edictors.pdf
Digital Tec...eholders.pdf
Electronic...urvivors .pdf
Exploring C...l Media.pdf
Feel what I...matters.pdf
Feminist Kil...ssange.pdf
How Tech i...iolence.pdf

Digital Technologies and Intimate Partner V...
641 KB

Created	03/03/2018, 10:52
Modified	03/03/2018, 10:52
Last opened	--

Add Tags...

Tech abuse research

- **Online harassment** (Winkelman, 2015; Aghazadeh et al., 2018)
- **Cyber stalking** (Pereira and Matos, 2016)
- **Spyware** (Chatterjee et al., 2018)
- **Image-based abuse / revenge porn / creepshots** (McGlynn, Rackley, Houghton, 2017; Powell et al., 2018)

SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

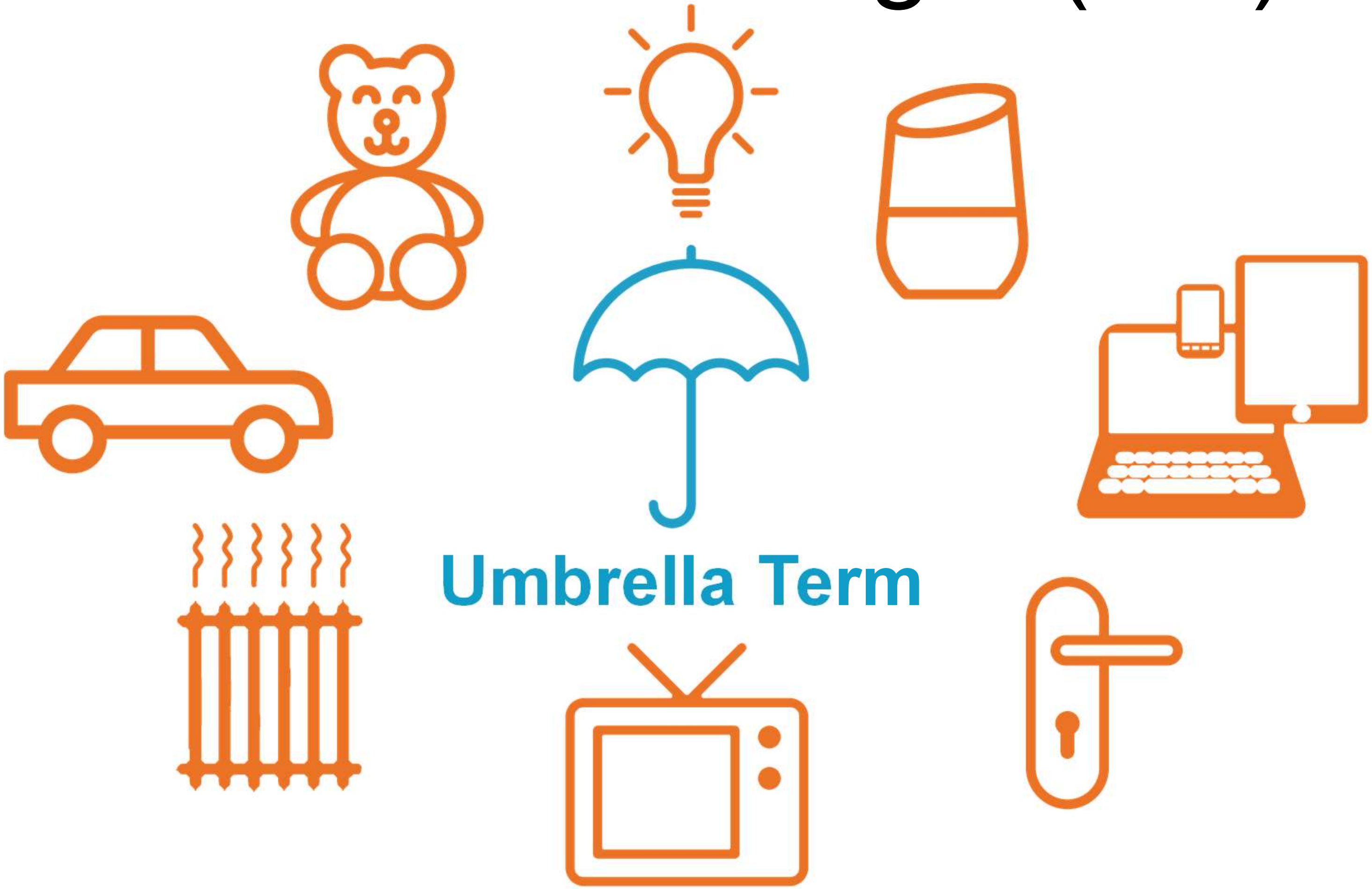
UCL

Technology is changing.

STE(a)PP
Applied in Focus. Global in Reach.

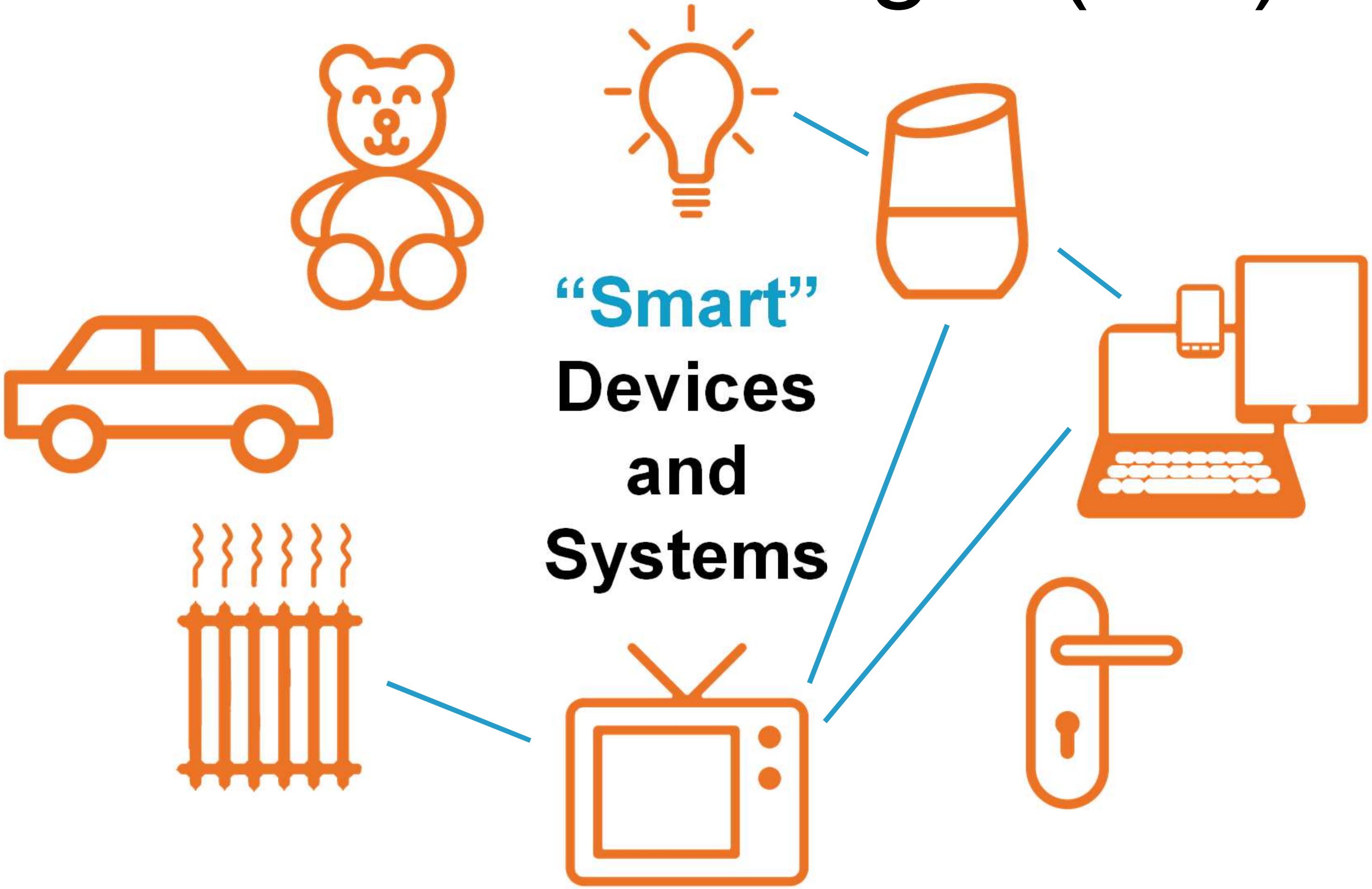
UCL ENGINEERING
Change the world

“Internet of Things” (IoT)?

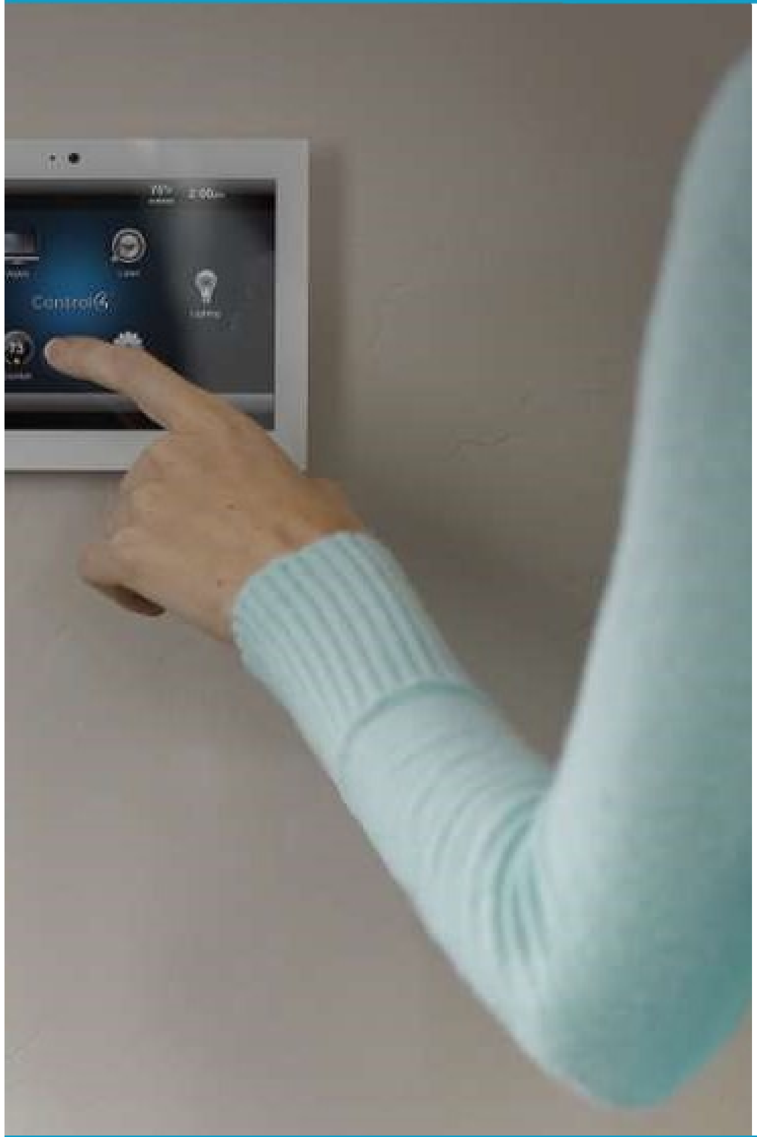


Umbrella Term

“Internet of Things” (IoT)?



“Smart” Devices and Systems



By 2020, some **25 billion devices** will be connected to the Internet with studies estimating that this number will rise to **125 billion in 2030**.

Tech abuse research

- **Online harassment** (Winkelman, 2015; Aghazadeh et al., 2018)
- **Cyber stalking** (Pereira and Matos, 2016)
- **Spyware** (Chatterjee et al., 2018)
- **Image-based abuse / revenge porn / creepshots** (McGlynn, Rackley, Houghton, 2017; Powell et al., 2018)

Phone, tablets, laptops, social media, CCTV, and trackers

“Smart” abuse?

Increasing number of 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

#GIoT Team

George Danezis

Leonie Tanczer

Isabel Lopez

Simon Parkin

Trupti Patel

Julia Slupska

SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

https://flic.kr/p/7mkGh9

Action Research

London VAWG Consortium

PETRAS

~~PRIVACY INTERNATIONAL~~

Department for Culture Media & Sport

National Cyber Security Centre
a part of GCHQ

STE[a]PP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world

G-IoT: aims

1. the **role and impact** IoT technologies have on victims/survivors of domestic violence and abuse;
2. the potential **risk trajectories** that may arise from those devices and services; and
3. the **awareness** victims/survivors and corresponding services (such as womens' shelters) exhibit, and strategies they apply to mitigate those risks.

https://flic.kr/p/4B8oJi

2 Workshops

6 Trainings

14 Interviews

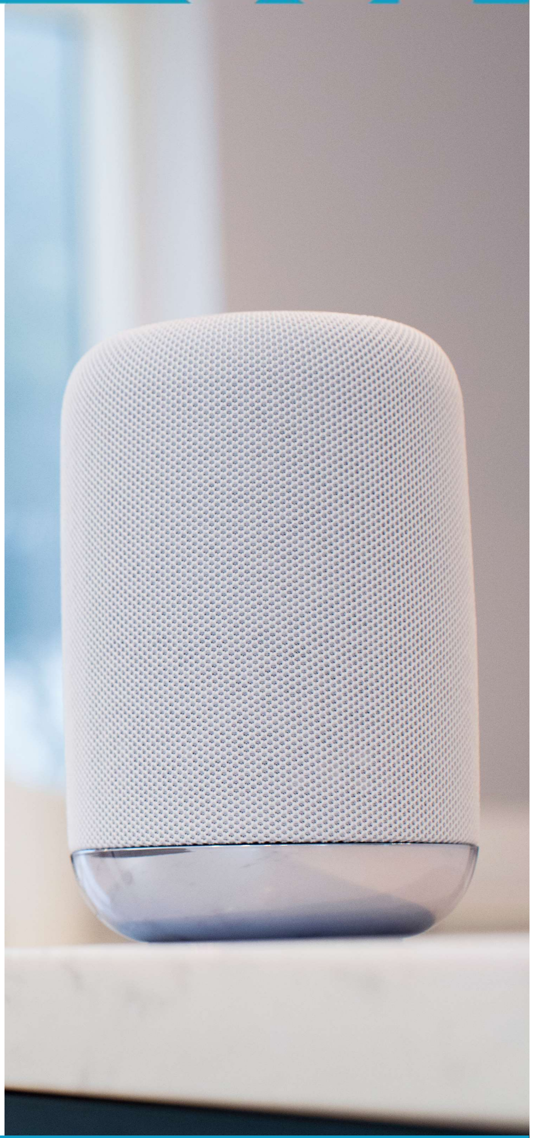
Tech analysis

1 CryptoParty

Outcomes

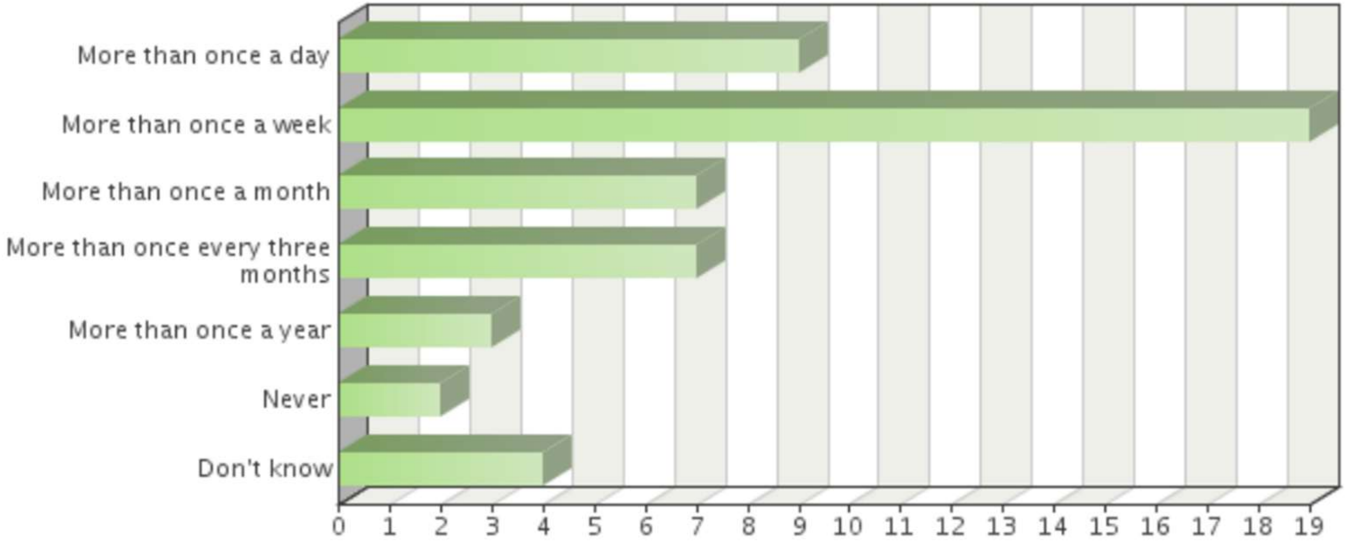
1. **Co-developed research** on the issue of emerging IoT risks
2. **Capacity-building** and knowledge exchange
3. **Transformative,** both in regards to practice and policy

(1)
Research



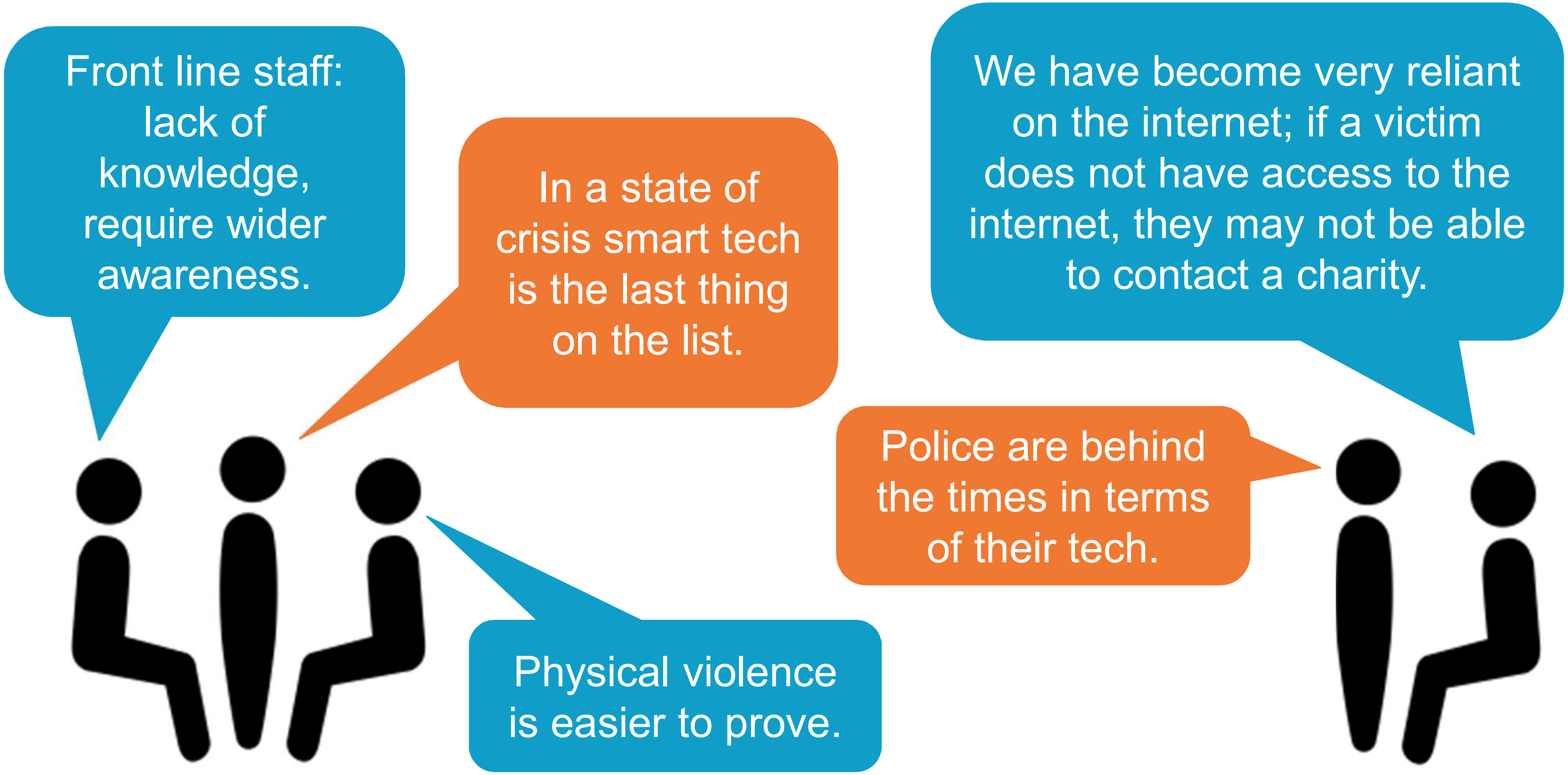
Question 2

How frequently do you encounter tech-related abuses when working within the area of victims/survivors of domestic and sexual violence and abuse?



n=51

Insights



Front line staff: lack of knowledge, require wider awareness.

In a state of crisis smart tech is the last thing on the list.

Physical violence is easier to prove.

We have become very reliant on the internet; if a victim does not have access to the internet, they may not be able to contact a charity.

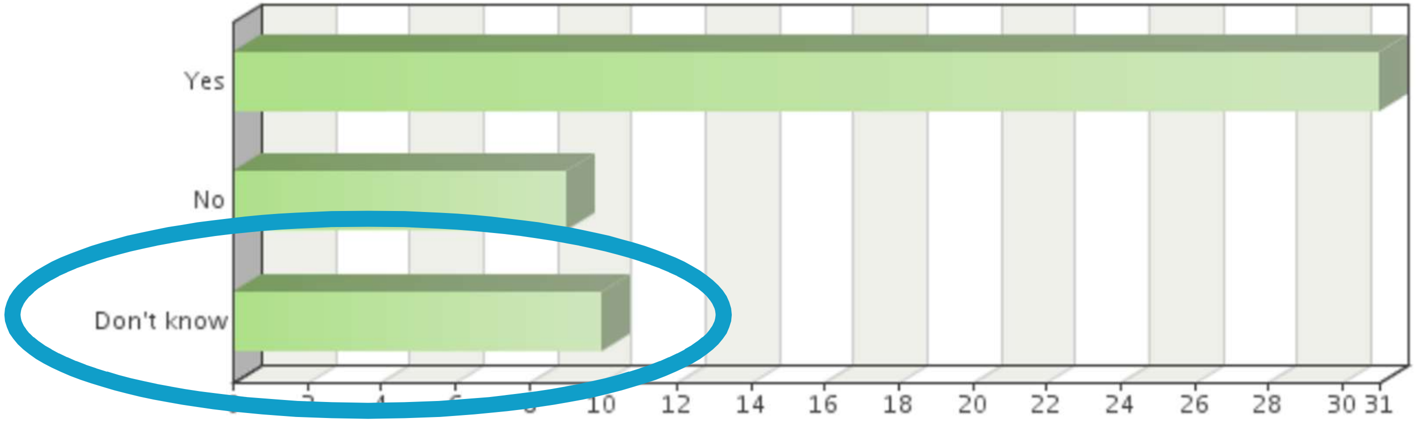
Police are behind the times in terms of their tech.

Positive impact

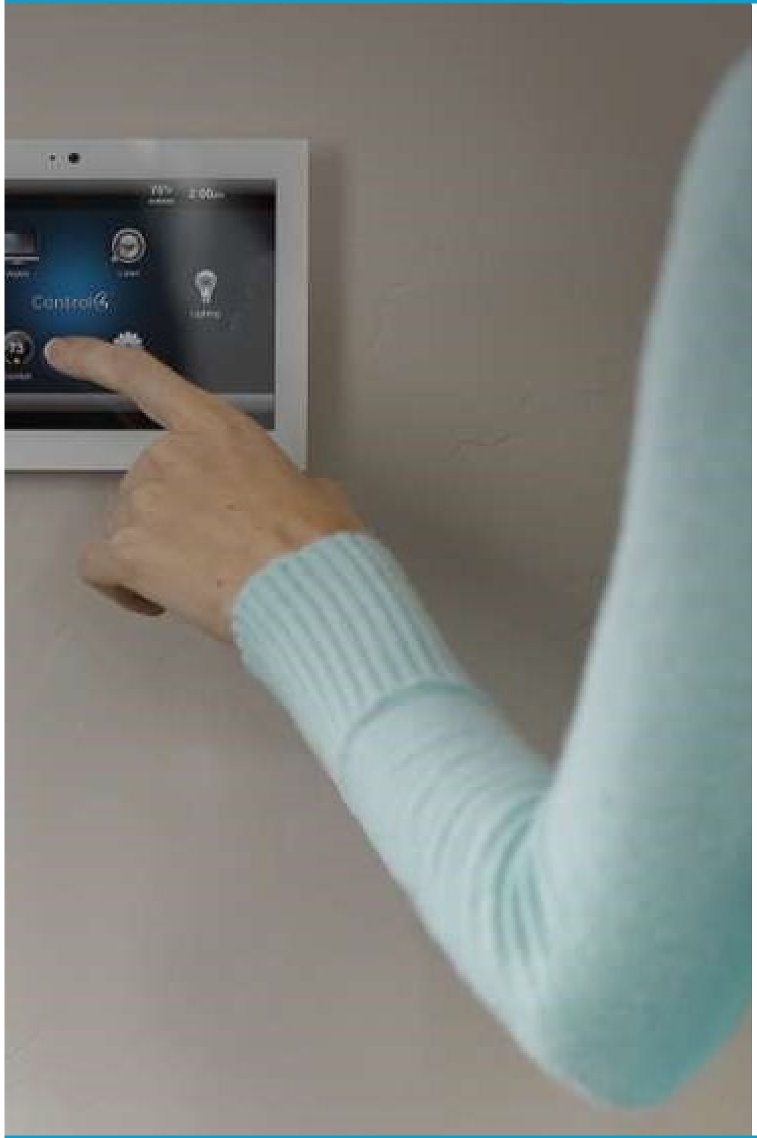
- **Logging of evidence** e.g., tampering, harassment
- **Video footage** e.g., CCTV
- **Communication and contact** e.g., seeking help
- **Online forums and bots** e.g., receiving advice and guidance
- **Detection**?
    - Empowerment

Question 4

Have you already experienced IoT technologies (i.e., "smart", Internet-connected devices) being of concern when working with victims/survivors of domestic and sexual violence and abuse?



n=50



Technical Analysis

1. Management
2. Assumptions
3. Usage

For example: Google Home

Settings and Activation

- Offers a "**Multi-User Support**", recognising different voices
- A Google account links to **other services**, e.g. Google Play, Netflix

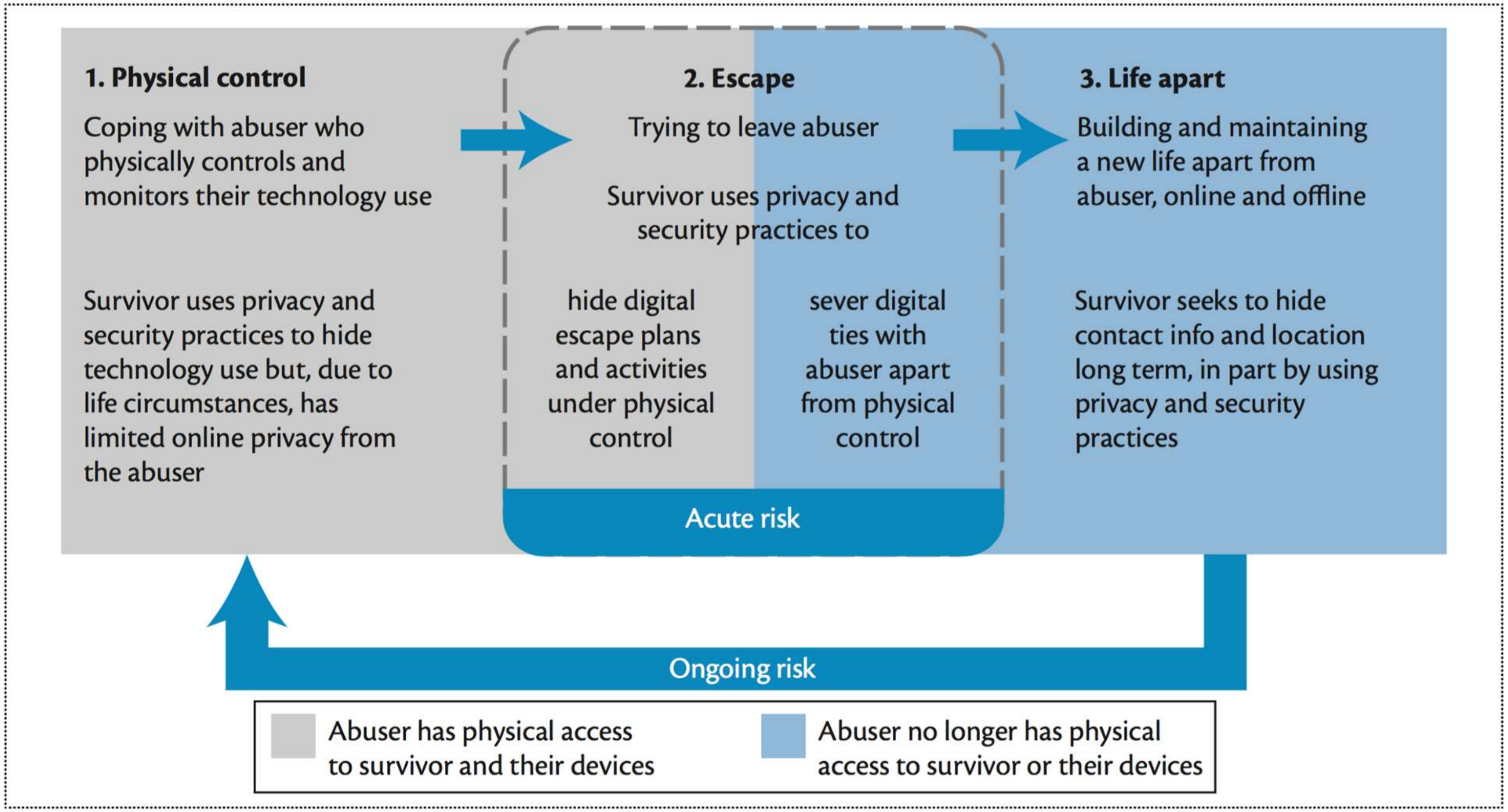
Data Collection

- Google Home collects **voice requests** and browsing history

Privacy and Security Considerations

- History and voice requests may be **deleted** by going to *myactivity.google.com*

IPA and Technology Use



1. Physical control

Coping with abuser who physically controls and monitors their technology use

Survivor uses privacy and security practices to hide technology use but, due to life circumstances, has limited online privacy from the abuser

2. Escape

Trying to leave abuser

Survivor uses privacy and security practices to

hide digital escape plans and activities under physical control

sever digital ties with abuser apart from physical control

Acute risk

3. Life apart

Building and maintaining a new life apart from abuser, online and offline

Survivor seeks to hide contact info and location long term, in part by using privacy and security practices

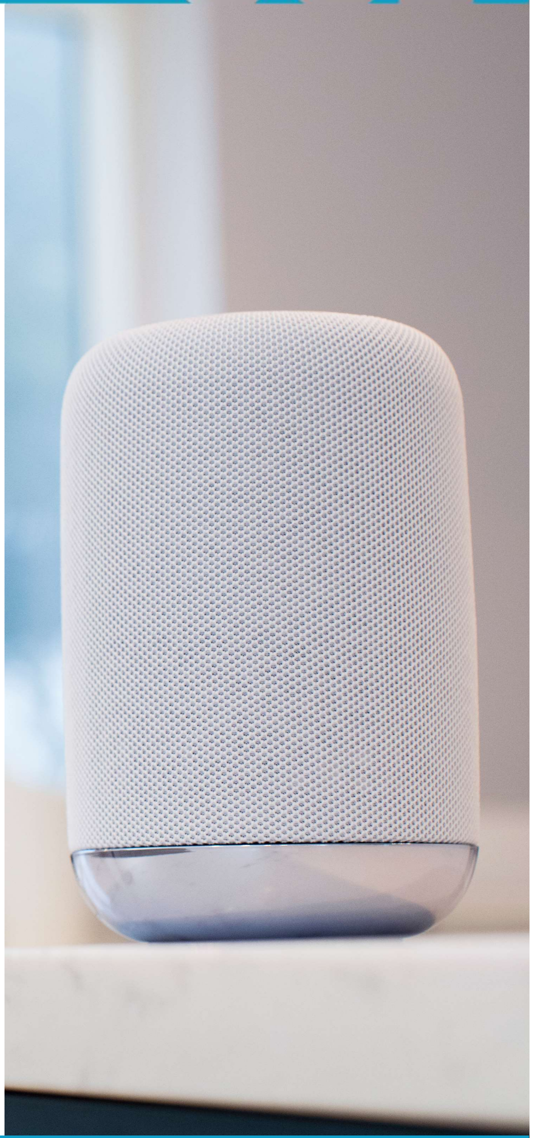
Ongoing risk

▨ Abuser has physical access to survivor and their devices

🟦 Abuser no longer has physical access to survivor or their devices

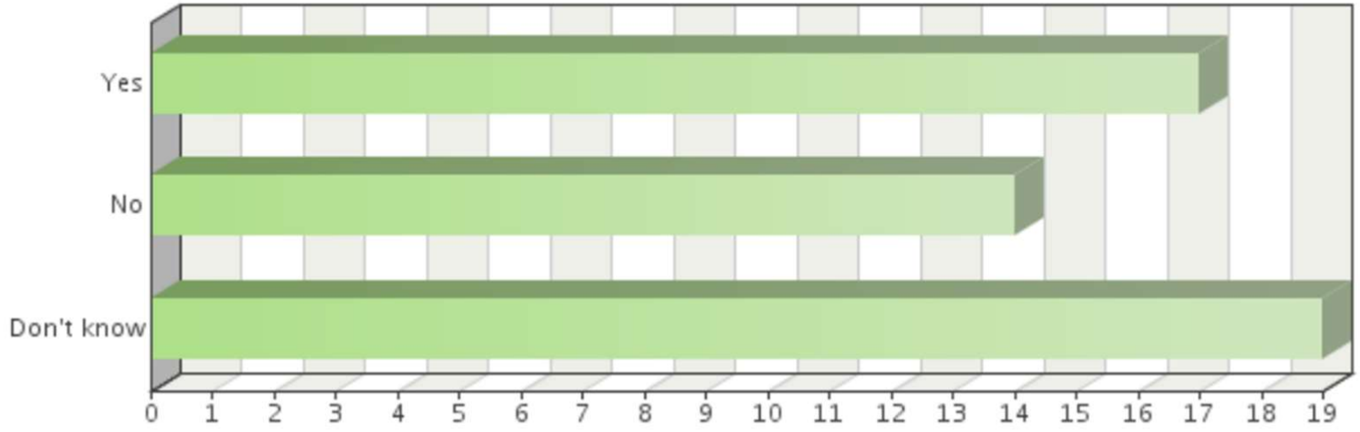
Matthews et al. 2017. Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse. CHI 2017.

(2)
Capacity Building



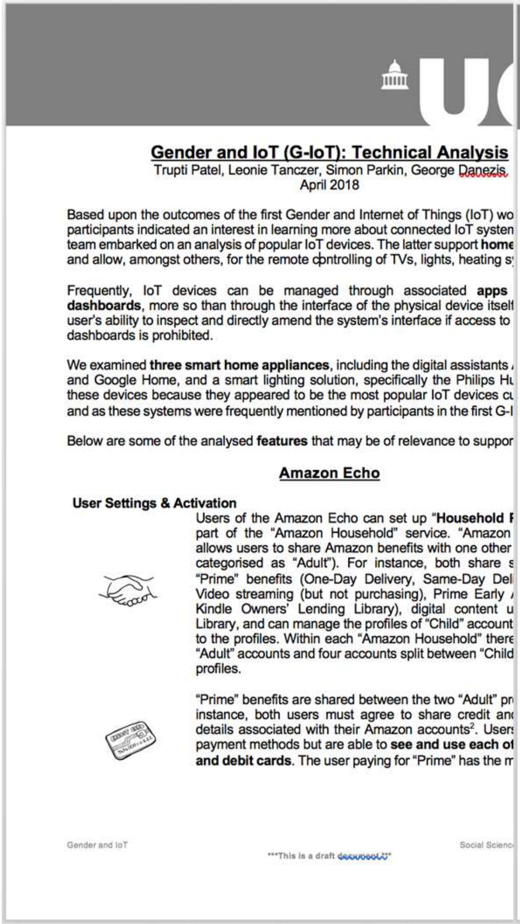
Question 8

Is your organisation documenting and categorising tech-related abuses?



n=50

Information Material



UC

Gender and IoT (G-IoT): Technical Analysis

Trupti Patel, Leonie Tanczer, Simon Parkin, George Danezis
April 2018

Based upon the outcomes of the first Gender and Internet of Things (IoT) wo
participants indicated an interest in learning more about connected IoT systen
team embarked on an analysis of popular IoT devices. The latter support **home**
and allow, amongst others, for the remote controlling of TVs, lights, heating s

Frequently, IoT devices can be managed through associated **apps**
dashboards, more so than through the interface of the physical device itsel
user's ability to inspect and directly amend the system's interface if access to
dashboards is prohibited.

We examined **three smart home appliances**, including the digital assistants
and Google Home, and a smart lighting solution, specifically the Philips Hu
these devices because they appeared to be the most popular IoT devices cu
and as these systems were frequently mentioned by participants in the first G-I

Below are some of the analysed **features** that may be of relevance to suppor

Amazon Echo

User Settings & Activation

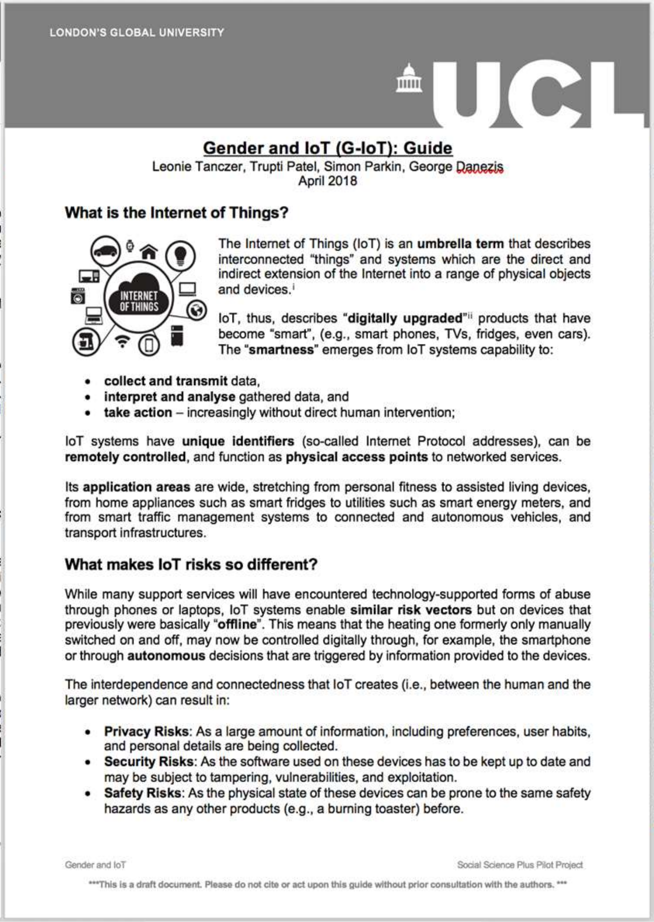
Users of the Amazon Echo can set up "**Household F**
part of the "Amazon Household" service. "Amazon
allows users to share Amazon benefits with one other
categorised as "Adult"). For instance, both share s
"Prime" benefits (One-Day Delivery, Same-Day Del
Video streaming (but not purchasing), Prime Early
Kindle Owners' Lending Library), digital content u
Library, and can manage the profiles of "Child" account
to the profiles. Within each "Amazon Household" there
"Adult" accounts and four accounts split between "Child
profiles.

"Prime" benefits are shared between the two "Adult" pr
instance, both users must agree to share credit and
details associated with their Amazon accounts[2]. Users
payment methods but are able to **see and use each of**
and debit cards. The user paying for "Prime" has the m

Gender and IoT

Social Scienc

This is a draft document.



LONDON'S GLOBAL UNIVERSITY

UCL

Gender and IoT (G-IoT): Guide

Leonie Tanczer, Trupti Patel, Simon Parkin, George Danezis
April 2018

What is the Internet of Things?

The Internet of Things (IoT) is an **umbrella term** that describes interconnected "things" and systems which are the direct and indirect extension of the Internet into a range of physical objects and devices.[i]

IoT, thus, describes "**digitally upgraded**"[ii] products that have become "smart", (e.g., smart phones, TVs, fridges, even cars). The "**smartness**" emerges from IoT systems capability to:

- **collect and transmit** data,
- **interpret and analyse** gathered data, and
- **take action** – increasingly without direct human intervention;

IoT systems have **unique identifiers** (so-called Internet Protocol addresses), can be **remotely controlled**, and function as **physical access points** to networked services.

Its **application areas** are wide, stretching from personal fitness to assisted living devices, from home appliances such as smart fridges to utilities such as smart energy meters, and from smart traffic management systems to connected and autonomous vehicles, and transport infrastructures.

What makes IoT risks so different?

While many support services will have encountered technology-supported forms of abuse through phones or laptops, IoT systems enable **similar risk vectors** but on devices that previously were basically "**offline**". This means that the heating one formerly only manually switched on and off, may now be controlled digitally through, for example, the smartphone or through **autonomous** decisions that are triggered by information provided to the devices.

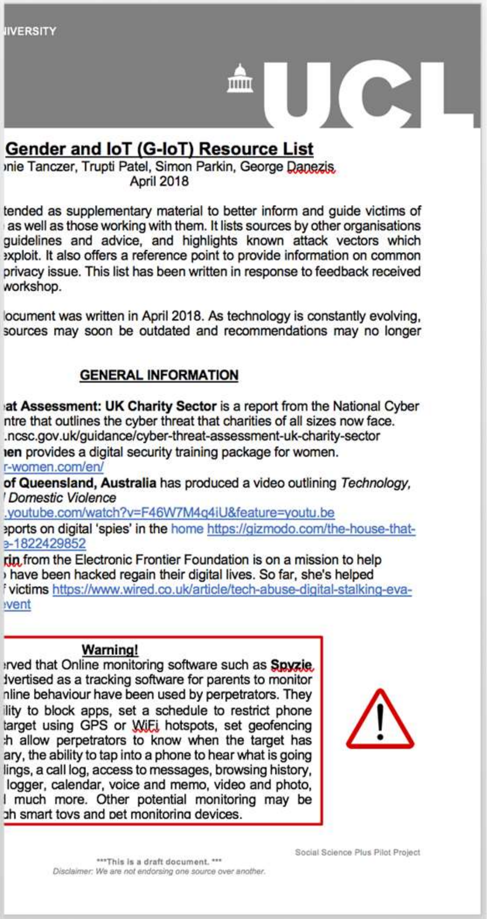
The interdependence and connectedness that IoT creates (i.e., between the human and the larger network) can result in:

- **Privacy Risks**: As a large amount of information, including preferences, user habits, and personal details are being collected.
- **Security Risks**: As the software used on these devices has to be kept up to date and may be subject to tampering, vulnerabilities, and exploitation.
- **Safety Risks**: As the physical state of these devices can be prone to the same safety hazards as any other products (e.g., a burning toaster) before.

Gender and IoT

Social Science Plus Pilot Project

***This is a draft document. Please do not cite or act upon this guide without prior consultation with the authors. ***



IVERSITY

UCL

Gender and IoT (G-IoT) Resource List

nie Tanczer, Trupti Patel, Simon Parkin, George Danezis
April 2018

tended as supplementary material to better inform and guide victims of
as well as those working with them. It lists sources by other organisations
guidelines and advice, and highlights known attack vectors which
xploit. It also offers a reference point to provide information on common
privacy issue. This list has been written in response to feedback received
workshop.

locument was written in April 2018. As technology is constantly evolving,
sources may soon be outdated and recommendations may no longer

GENERAL INFORMATION

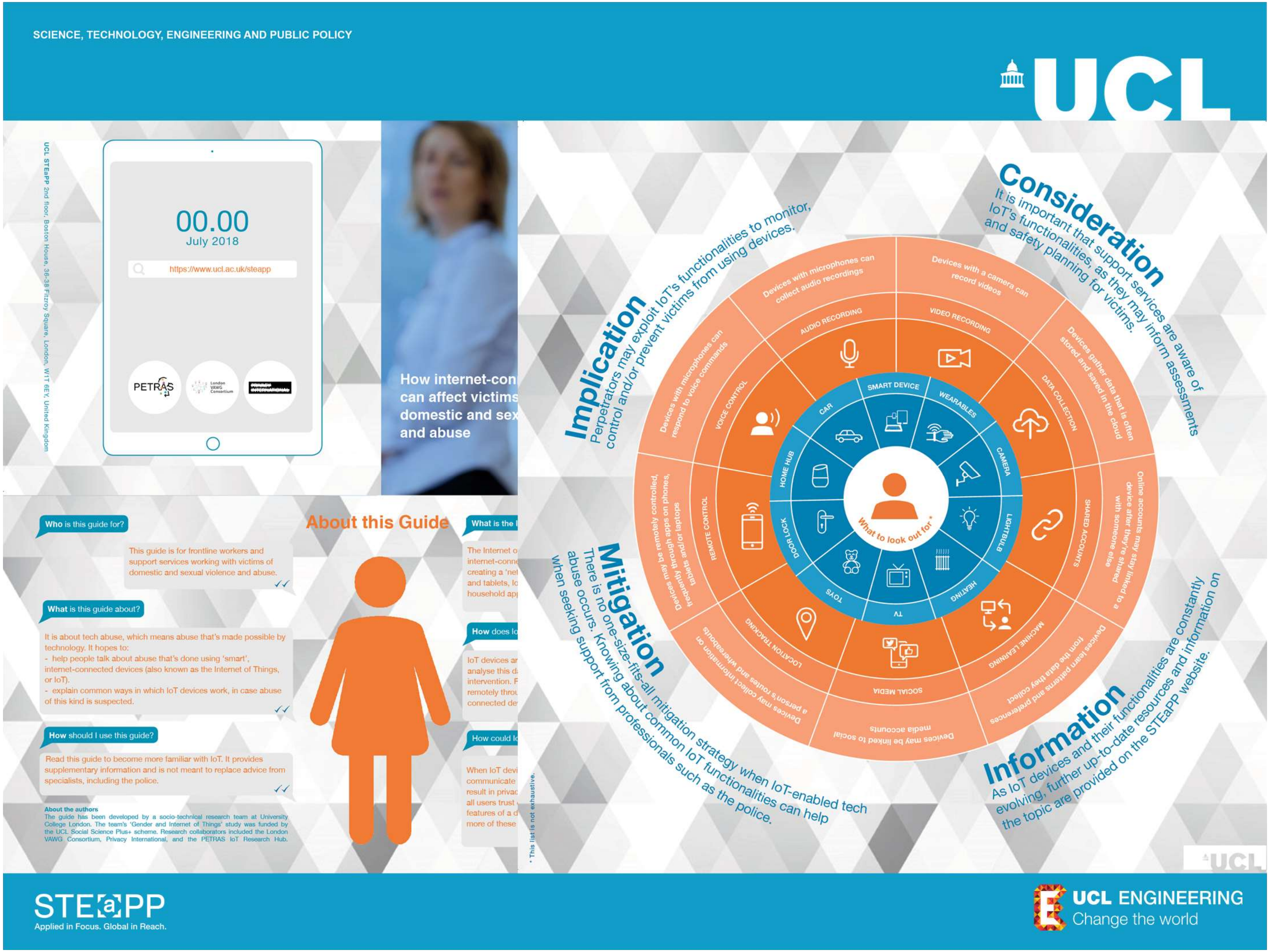
at Assessment: UK Charity Sector is a report from the National Cyber
ntre that outlines the cyber threat that charities of all sizes now face.
.ncsc.gov.uk/guidance/cyber-threat-assessment-uk-charity-sector
ien provides a digital security training package for women.
r-women.com/en/
of Queensland, Australia has produced a video outlining *Technology,*
Domestic Violence
.youtube.com/watch?v=F46W7M4q4iU&feature=youtu.be
eports on digital 'spies' in the home https://gizmodo.com/the-house-that-
e-1822429852
rin from the Electronic Frontier Foundation is on a mission to help
have been hacked regain their digital lives. So far, she's helped
victims https://www.wired.co.uk/article/tech-abuse-digital-stalking-eva-
vent

Warning!

rved that Online monitoring software such as **Spyzie**
dvertised as a tracking software for parents to monitor
nline behaviour have been used by perpetrators. They
ility to block apps, set a schedule to restrict phone
target using GPS or WiFi hotspots, set geofencing
h allow perpetrators to know when the target has
ary, the ability to tap into a phone to hear what is going
lings, a call log, access to messages, browsing history,
logger, calendar, voice and memo, video and photo,
much more. Other potential monitoring may be
gh smart toys and pet monitoring devices.

Social Science Plus Pilot Project

***This is a draft document. ***
Disclaimer: We are not endorsing one source over another.



SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

UCL STEaPP 2nd floor, Boston House, 36-38 Fitzroy Square, London, W1T 6EY, United Kingdom

00.00
July 2018

https://www.ucl.ac.uk/steapp

How internet-con
can affect victims
domestic and sex
and abuse

About this Guide

Who is this guide for?

This guide is for frontline workers and support services working with victims of domestic and sexual violence and abuse. ✓✓

What is this guide about?

It is about tech abuse, which means abuse that's made possible by technology. It hopes to:
- help people talk about abuse that's done using 'smart', internet-connected devices (also known as the Internet of Things, or IoT).
- explain common ways in which IoT devices work, in case abuse of this kind is suspected. ✓✓

How should I use this guide?

Read this guide to become more familiar with IoT. It provides supplementary information and is not meant to replace advice from specialists, including the police. ✓✓

About the authors
The guide has been developed by a socio-technical research team at University College London. The team's 'Gender and Internet of Things' study was funded by the UCL Social Science Plus+ scheme. Research collaborators included the London VAWG Consortium, Privacy International, and the PETRAS IoT Research Hub.

What is the I

The Internet o
internet-conne
creating a 'ne
and tablets, lo
household ap

How does Io

IoT devices ar
analyse this d
intervention. F
remotely throu
connected de

How could Io

When IoT devi
communicate
result in privac
all users trust
features of a d
more of these

Implication

Perpetrators may exploit IoT's functionalities to monitor, control and/or prevent victims from using devices.

Consideration

It is important that support services are aware of IoT's functionalities, as they may inform assessments and safety planning for victims.

Mitigation

There is no one-size-fits-all mitigation strategy when IoT-enabled tech abuse occurs. Knowing about common IoT functionalities can help when seeking support from professionals such as the police.

Information

As IoT devices and their functionalities are constantly evolving, further up-to-date resources and information on the topic are provided on the STEaPP website.

What to look out for *

SMART DEVICE
WEARABLES
CAMERA
LIGHTBULB
HEATING
TV
TOYS
DOOR LOCK
HOME HUB
CAR

AUDIO RECORDING
Devices with microphones can collect audio recordings

VIDEO RECORDING
Devices with a camera can record videos

DATA COLLECTION
Devices gather data that is often stored and saved in the cloud

SHARED ACCOUNTS
Online accounts may stay linked to a device after they're shared with someone else

MACHINE LEARNING
Devices learn patterns and preferences from the data they collect

SOCIAL MEDIA
Devices may be linked to social media accounts

LOCATION TRACKING
Devices may collect information on a person's routes and whereabouts

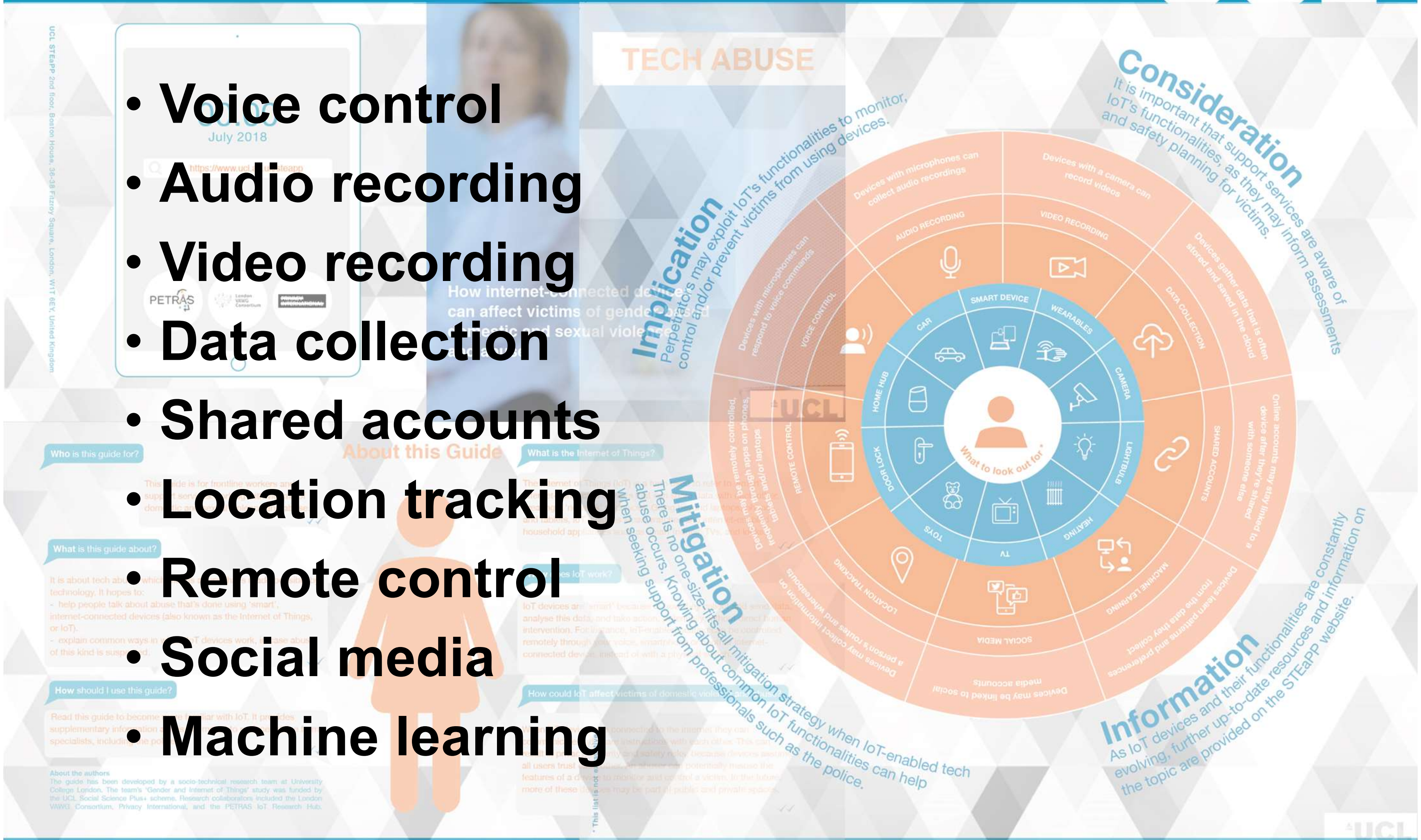
REMOTE CONTROL
Devices may be remotely controlled, frequently through apps on phones, tablets and/or laptops

VOICE CONTROL
Devices with microphones can respond to voice commands

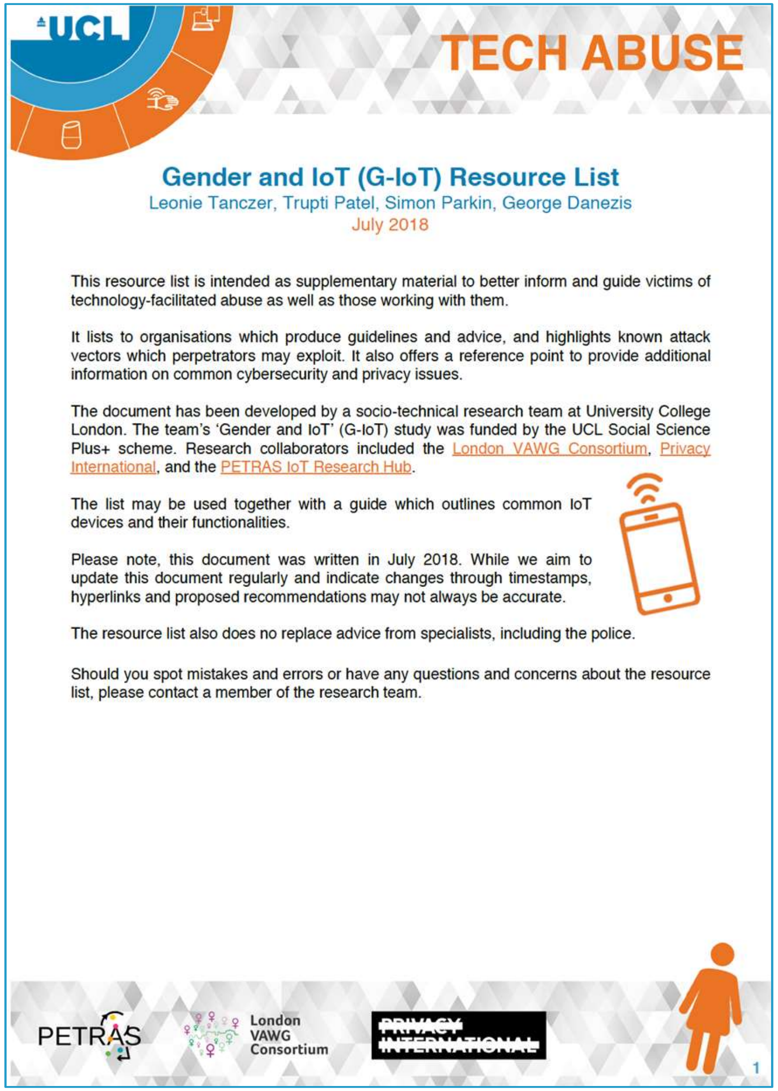
* This list is not exhaustive.

STE[a]PP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world


TECH ABUSE
July 2018
Consideration
It is important that support services are aware of IoT's functionalities, as they may inform assessments and safety planning for victims.
Implication
Perpetrators may exploit IoT's functionalities to monitor, control and/or prevent victims from using devices.
Mitigation
There is no one-size-fits-all mitigation strategy when IoT-enabled tech abuse occurs. Knowing about common IoT functionalities can help when seeking support from professionals such as the police.
Information
As IoT devices and their functionalities are constantly evolving, further up-to-date resources and information on the topic are provided on the STEaPP website.
What to look out for *
SMART DEVICE
WEARABLES
CAMERA
LIGHTBULB
HEATING
TV
TOYS
DOOR LOCK
HOME HUB
CAR
AUDIO RECORDING
VIDEO RECORDING
DATA COLLECTION
SHARED ACCOUNTS
MACHINE LEARNING
SOCIAL MEDIA
LOCATION TRACKING
REMOTE CONTROL
VOICE CONTROL

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



Gender and IoT (G-IoT) Resource List

Leonie Tanczer, Trupti Patel, Simon Parkin, George Danezis
July 2018

This resource list is intended as supplementary material to better inform and guide victims of technology-facilitated abuse as well as those working with them.

It lists to organisations which produce guidelines and advice, and highlights known attack vectors which perpetrators may exploit. It also offers a reference point to provide additional information on common cybersecurity and privacy issues.

The document has been developed by a socio-technical research team at University College London. The team's 'Gender and IoT' (G-IoT) study was funded by the UCL Social Science Plus+ scheme. Research collaborators included the London VAWG Consortium, Privacy International, and the PETRAS IoT Research Hub.

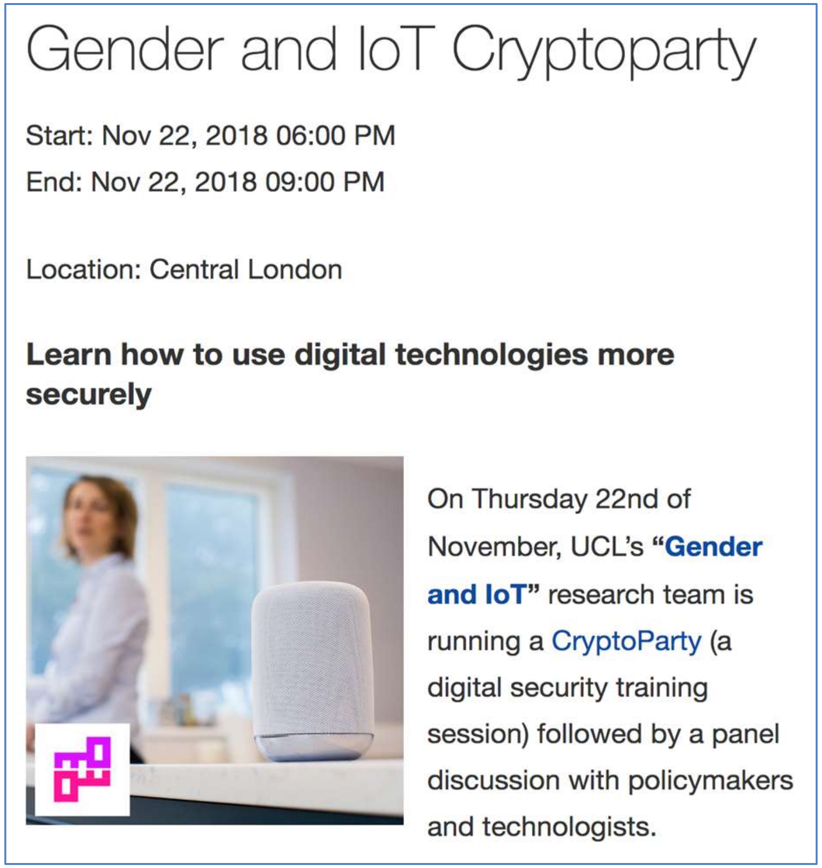
The list may be used together with a guide which outlines common IoT devices and their functionalities.

Please note, this document was written in July 2018. While we aim to update this document regularly and indicate changes through timestamps, hyperlinks and proposed recommendations may not always be accurate.

The resource list also does no replace advice from specialists, including the police.

Should you spot mistakes and errors or have any questions and concerns about the resource list, please contact a member of the research team.

Training



Gender and IoT Cryptoparty

Start: Nov 22, 2018 06:00 PM

End: Nov 22, 2018 09:00 PM

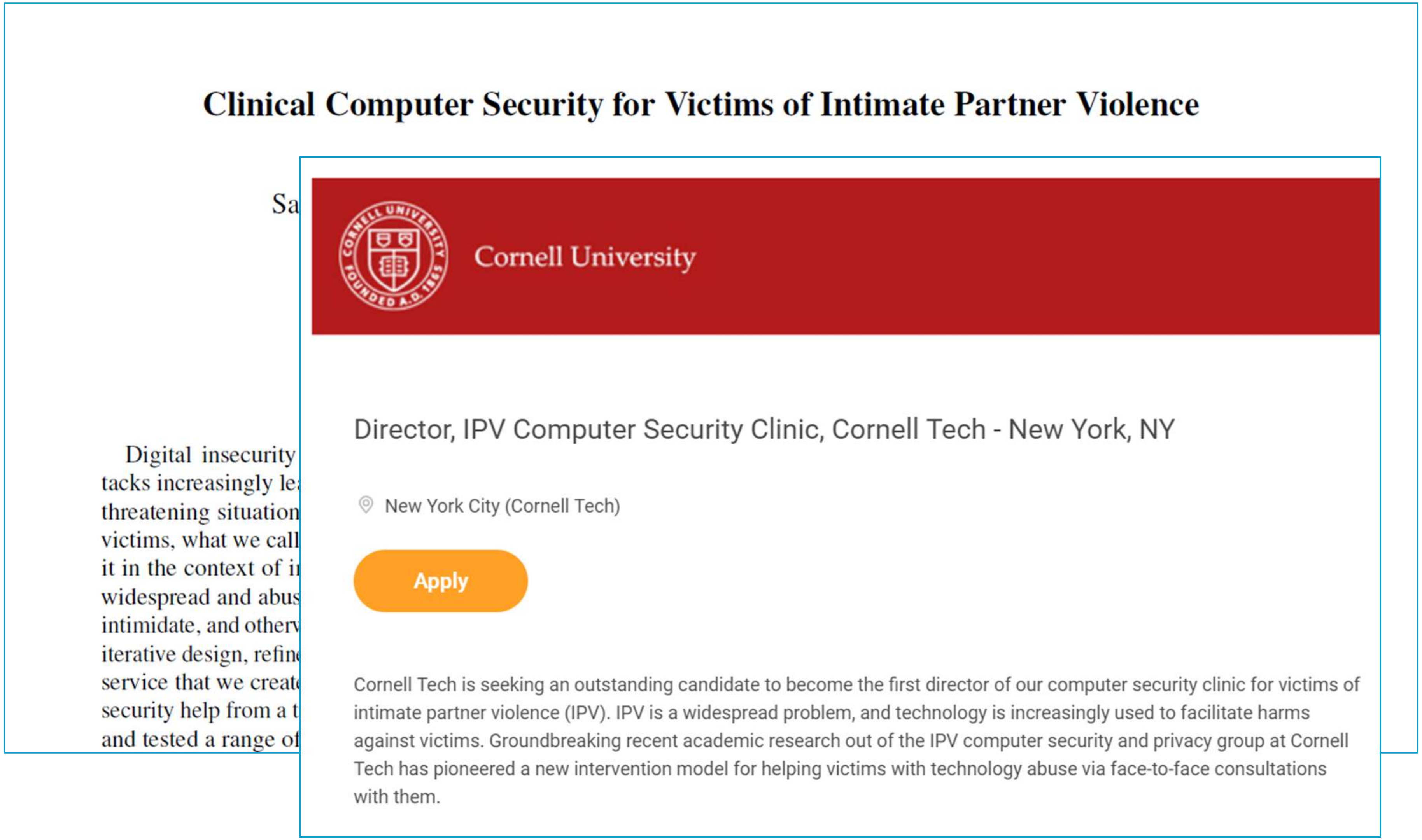
Location: Central London

Learn how to use digital technologies more securely

On Thursday 22nd of November, UCL's **"Gender and IoT"** research team is running a CryptoParty (a digital security training session) followed by a panel discussion with policymakers and technologists.

- CryptoParty: **Digital security training** for voluntary and statutory services

- Information exchange **workshops** for voluntary and statutory services frontline workers and support organisations



Clinical Computer Security for Victims of Intimate Partner Violence

Sa

Digital insecurity
tacks increasingly le
threatening situation
victims, what we call
it in the context of i
widespread and abus
intimidate, and other
iterative design, refin
service that we create
security help from a t
and tested a range of

Cornell University

Director, IPV Computer Security Clinic, Cornell Tech - New York, NY

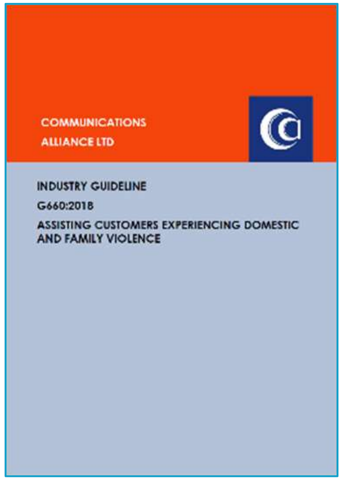
New York City (Cornell Tech)

Apply

Cornell Tech is seeking an outstanding candidate to become the first director of our computer security clinic for victims of intimate partner violence (IPV). IPV is a widespread problem, and technology is increasingly used to facilitate harms against victims. Groundbreaking recent academic research out of the IPV computer security and privacy group at Cornell Tech has pioneered a new intervention model for helping victims with technology abuse via face-to-face consultations with them.

Pointers for industry

- **Prompts and notifications** (e.g., location tracking on, what devices want to connect)
- **Logs** (e.g., who has connected to what, when)
- **IPV threat model** (e.g., trust levels)
- **Customer-facing staff guidance** (e.g., helplines, shop workers)
- **Data collection** (e.g., extent of the problem and what types of requests)
- **Exchange and collaboration with support sector** (e.g., data and remediation)



COMMUNICATIONS ALLIANCE LTD

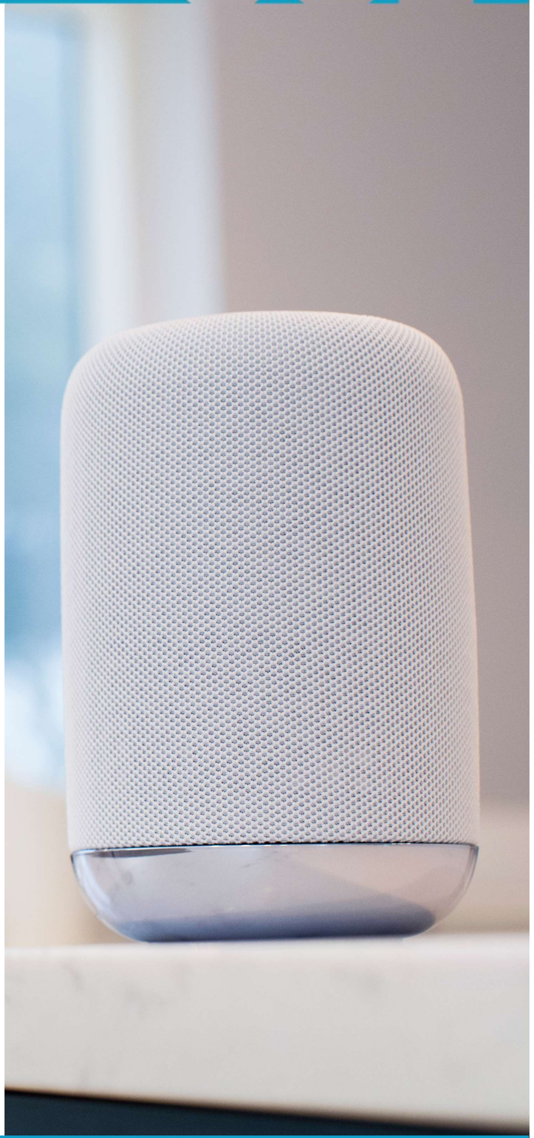
INDUSTRY GUIDELINE

G660:2018

ASSISTING CUSTOMERS EXPERIENCING DOMESTIC AND FAMILY VIOLENCE

https://commsalliance.com.au/__data/assets/pdf_file/0003/61527/Communications-Guideline-G660-Assisting-Customers-Experiencing-Domestic-and-Family-Violence.pdf

(3)
Transformation



SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

Responsibility

STE@PP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world

SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

Industry

Politics

Society

STE@PP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world

UK Government Consultation

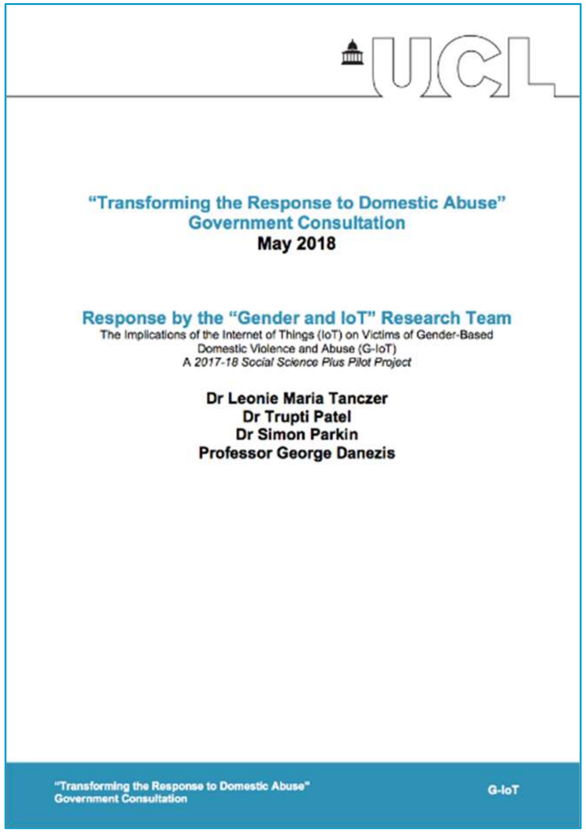
(1) Tech abuse as a factor in the **risk assessment** of victims;

(2) Tech abuse as a factor in the **safety planning** of victims;

(3) Expand the focus on tech abuse to emerging technologies such as the **Internet of Things**;

(4) Create tech abuse **guidance and expertise**;

(5) Reduce/remove prevalence of **spyware**;



UCL

"Transforming the Response to Domestic Abuse"
Government Consultation
May 2018

Response by the "Gender and IoT" Research Team
The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT)
A 2017-18 Social Science Plus Pilot Project

Dr Leonie Maria Tanczer
Dr Trupti Patel
Dr Simon Parkin
Professor George Danezis

"Transforming the Response to Domestic Abuse"
Government Consultation

G-IoT

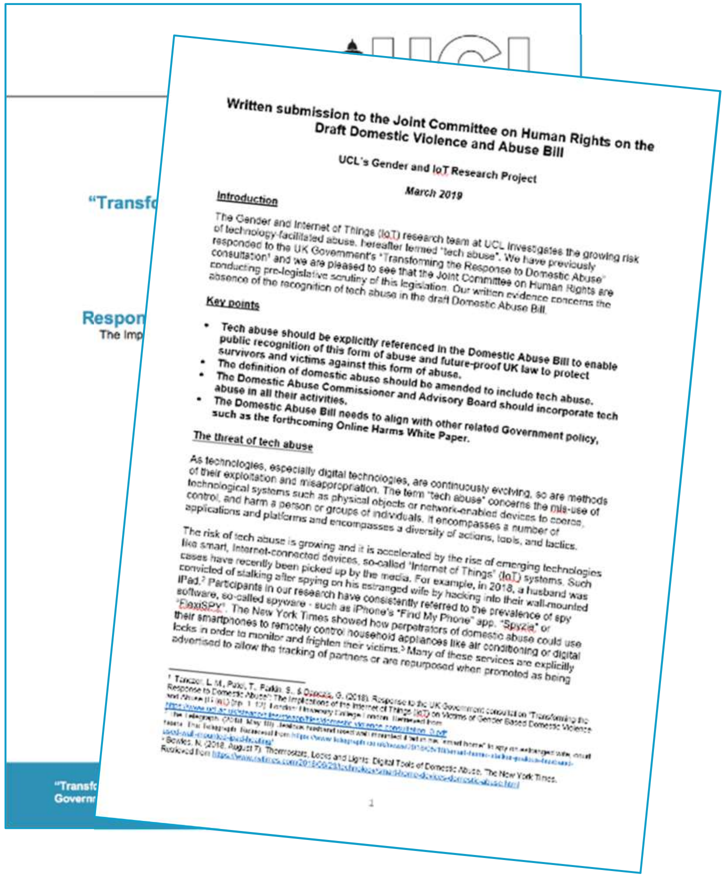
UK Government Consultation

(1) Tech abuse should be **explicitly referenced** in the Domestic Abuse Bill to enable public recognition

(2) The **definition** of domestic abuse should be amended to include tech abuse;

(3) The Domestic Abuse **Commissioner and Advisory Board** should incorporate tech abuse in all their activities;

(4) Align with other **related Government policy**;



UCL

“Transfo

Respon
The Imp

“Transfo
Govern

Written submission to the Joint Committee on Human Rights on the Draft Domestic Violence and Abuse Bill

UCL's Gender and IoT Research Project

March 2019

Introduction

The Gender and Internet of Things (IoT) research team at UCL investigates the growing risk of technology-facilitated abuse, hereafter termed "tech abuse". We have previously responded to the UK Government's "Transforming the Response to Domestic Abuse" consultation[1] and we are pleased to see that the Joint Committee on Human Rights are conducting pre-legislative scrutiny of this legislation. Our written evidence concerns the absence of the recognition of tech abuse in the draft Domestic Abuse Bill.

Key points

- **Tech abuse should be explicitly referenced in the Domestic Abuse Bill to enable public recognition of this form of abuse and future-proof UK law to protect survivors and victims against this form of abuse.**
- **The definition of domestic abuse should be amended to include tech abuse.**
- **The Domestic Abuse Commissioner and Advisory Board should incorporate tech abuse in all their activities.**
- **The Domestic Abuse Bill needs to align with other related Government policy, such as the forthcoming Online Harms White Paper.**

The threat of tech abuse

As technologies, especially digital technologies, are continuously evolving, so are methods of their exploitation and misappropriation. The term "tech abuse" concerns the mis-use of technological systems such as physical objects or network-enabled devices to coerce, control, and harm a person or groups of individuals. It encompasses a number of applications and platforms and encompasses a diversity of actions, tools, and tactics.

The risk of tech abuse is growing and it is accelerated by the rise of emerging technologies like smart, Internet-connected devices, so-called "Internet of Things" (IoT) systems. Such cases have recently been picked up by the media. For example, in 2018, a husband was convicted of stalking after spying on his estranged wife by hacking into their wall-mounted iPad.[2] Participants in our research have consistently referred to the prevalence of spy software, so-called spyware - such as iPhone's "Find My Phone" app, "Spyzie" or "FlexiSPY". The New York Times showed how perpetrators of domestic abuse could use their smartphones to remotely control household appliances like air conditioning or digital locks in order to monitor and frighten their victims.[3] Many of these services are explicitly advertised to allow the tracking of partners or are repurposed when promoted as being

[1] Tanczer, L. M., Patel, T., Parkin, S., & Danezis, G. (2018). Response to the UK Government consultation "Transforming the Response to Domestic Abuse": The Implications of the Internet of Things (IoT) on Victims of Gender Based Domestic Violence and Abuse (G-IoT) (pp. 1–12). London: University College London. Retrieved from [illegible]

[2] The Telegraph. (2018, May [illegible]). Jealous husband used wall-mounted iPad in the "smart home" to spy on estranged wife, court hears. The Telegraph. Retrieved from https://www.telegraph.co.uk/news/2018/05/[illegible]

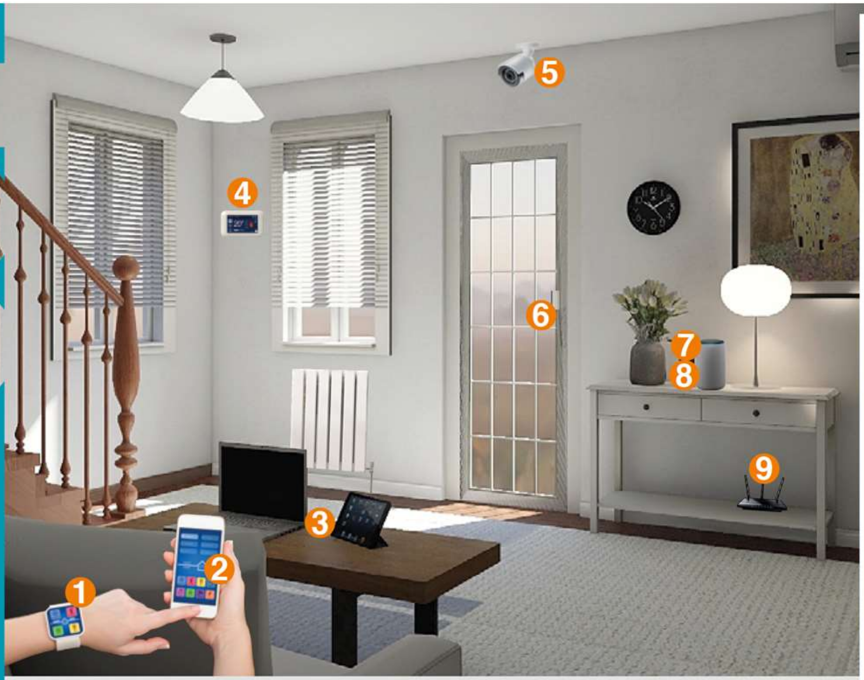
[3] Bowles, N. (2018, August 7). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. The New York Times. Retrieved from https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

1

SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

UCL

DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY



Tech Abuse – Smart, Internet-connected de risks for victims of domestic

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.

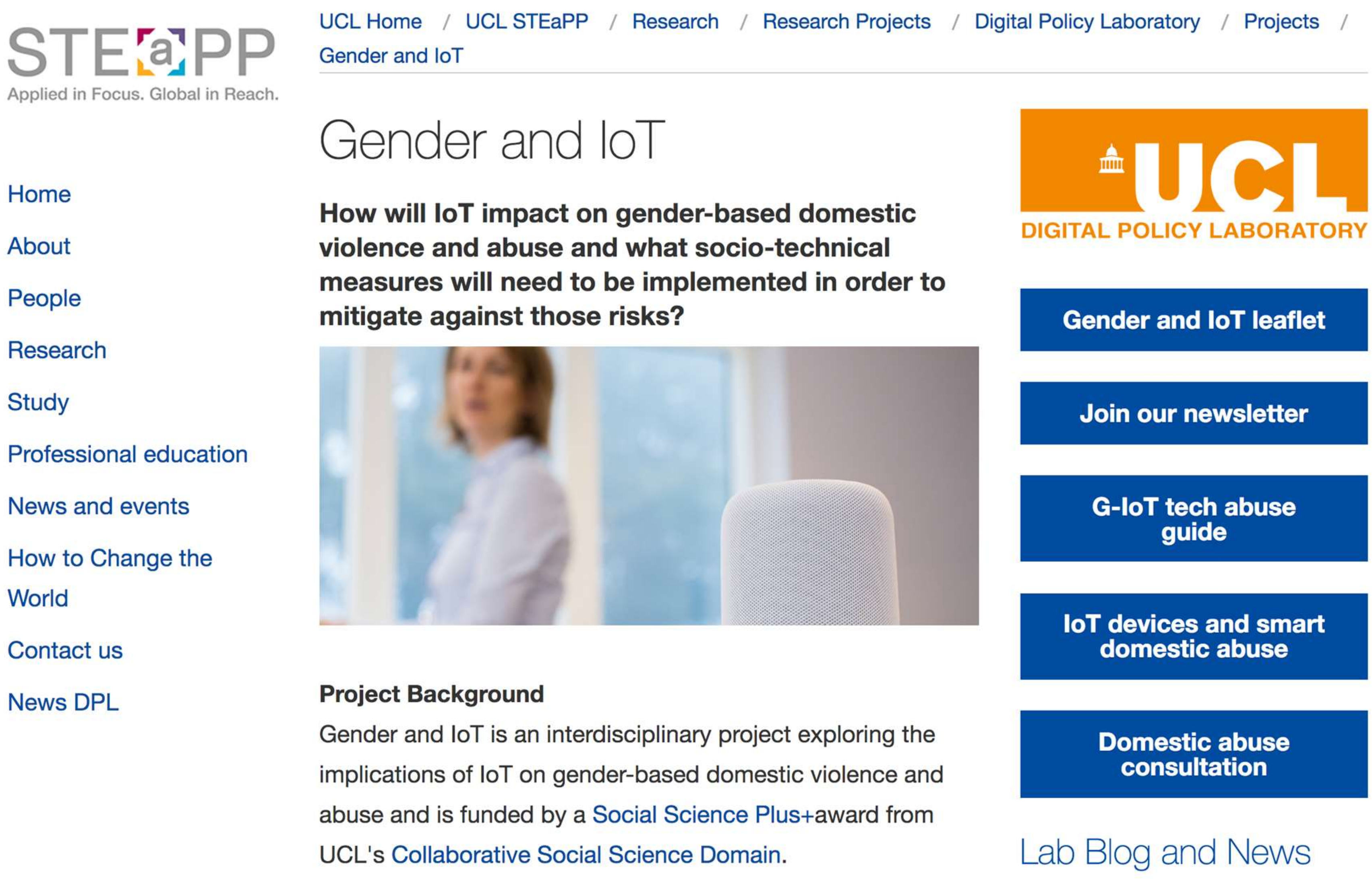
4 Remote control of heating, lighting and blinds
Could be used to coerce and intimidate victims by switching systems on or off from afar.

Recommendations

1. **Internet security legislation must be 'future-proofed'** against the expected growth in the number of Internet-connected home devices.
2. **Capacity to deal with the threat of tech-abuse needs to be available at the front line.** This requires training for front-line staff and access to technical expertise, for example via a dedicated hotline. Police forces also need to be better equipped to deal with this form of abuse.
3. The risk of tech abuse must be incorporated into **risk assessment and safety planning processes**.
4. **More data is needed to understand the scale of the problem and to monitor changes over time.** Police and frontline staff need to change their reporting patterns to achieve this.

STEaPP
Applied in Focus. Global in Reach.

UCL ENGINEERING
Change the world



UCL Home / UCL STEaPP / Research / Research Projects / Digital Policy Laboratory / Projects / Gender and IoT

STE(a)PP
Applied in Focus. Global in Reach.

- Home
- About
- People
- Research
- Study
- Professional education
- News and events
- How to Change the World
- Contact us
- News DPL

Gender and IoT

How will IoT impact on gender-based domestic violence and abuse and what socio-technical measures will need to be implemented in order to mitigate against those risks?

Project Background

Gender and IoT is an interdisciplinary project exploring the implications of IoT on gender-based domestic violence and abuse and is funded by a Social Science Plus+award from UCL's Collaborative Social Science Domain.

UCL DIGITAL POLICY LABORATORY

- Gender and IoT leaflet
- Join our newsletter
- G-IoT tech abuse guide
- IoT devices and smart domestic abuse
- Domestic abuse consultation

Lab Blog and News

Thank you.

Dr Leonie Tanczer
l.tanczer@ucl.ac.uk

Twitter: @leotanczt, #GIoT

References and further reading

- Currah, P., & Mulqueen, T. (2011). *Securitizing Gender: Identity, Biometrics, and Transgender Bodies at the Airport* (p. 27). New York: CUNY Academic Works. Retrieved from https://academicworks.cuny.edu/cgi/viewcontent.cgi?article=1334&context=gc_pubs
- Rakow, L. F. (1988). Gendered technology, gendered practice. *Critical Studies in Mass Communication*, *5*(1), 57–70. https://doi.org/10.1080/15295038809366685
- Bose, D., Segui-Gomez, M., & Crandall, J. R. (2011). Vulnerability of Female Drivers Involved in Motor Vehicle Crashes: An Analysis of US Population at Risk. *American Journal of Public Health*, *101*(12), 2368–2373. https://doi.org/10.2105/AJPH.2011.300275
- Cowan, R. S. (1983). *More work for mother: the ironies of household technology from the open hearth to the microwave.* New York: Basic Books.
- Kaiser, A. (2010). Sex/gender and neuroscience: focusing on current research. In M. Blomqvist & E. Ehnsmyr (Eds.), *Never Mind the Gap! Crossroads of Knowledge* (Vol. 14, pp. 189–210). Uppsala: Centre for Gender Research.

References and further reading

- West, C., & Zimmerman, D. H. (1987). Doing gender. In S. A. Farrell J. .. Lorber (Ed.) (Vol. 1, pp. 125–151). Newbury Park & London: Sage Publications.
- Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., … Ristenpart, T. (2018). The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)* (pp. 993–1010). https://doi.org/10.1109/SP.2018.00061
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, *25*(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2
- Powell, A., Henry, N., Flynn, A., Scott, A.J. (2018). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian adults, *Computers in Human Behavior*, doi: 10.1016/j.chb.2018.11.009
- Pereira, F., & Matos, M. (2016). Cyber-Stalking Victimization: What Predicts Fear Among Portuguese Adolescents? *European Journal on Criminal Policy and Research*, *22*(2), 253–270. https://doi.org/10.1007/s10610-015-9285-7

References and further reading

- Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring Cyber Harrassment among Women Who Use Social Media. *Universal Journal of Public Health*, *3*(5), 194–201. https://doi.org/10.13189/ujph.2015.030504
- Aghazadeh, S. A., Burns, A., Chu, J., Feigenblatt, H., Laribee, E., Maynard, L., … Rufus, L. (2018). GamerGate: A Case Study in Online Harassment. In J. Golbeck (Ed.), *Online Harassment* (pp. 179–207). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-78583-7_8
- Light, B., Burgess, J., & Duguay, S. (2018). The walkthrough method: An approach to the study of apps. *New Media & Society*, *20*(3), 881–900. https://doi.org/10.1177/1461444816675438
- 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. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 2189–2201). New York, NY, USA: ACM. https://doi.org/10.1145/3025453.3025875