TECH ABUSE

How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse

UCL

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 Internet of Things?

The Internet of Things (IoT) is a term used to refer to 'smart', internet-connected devices that can share data with each other, creating a 'network' of devices. Going beyond laptops, phones and tablets, IoT includes smart watches and internet-enabled household appliances such as smart fridges, TVs, and locks.

How does IoT work?

IoT devices are 'smart' because of how they collect and send data, analyse this data, and take action, potentially without direct human intervention. For instance, IoT-enabled heating can be controlled remotely through your voice, smartphone or another internet-connected device, instead of with a physical switch.

How could IoT **affect victims** of domestic violence and abuse?

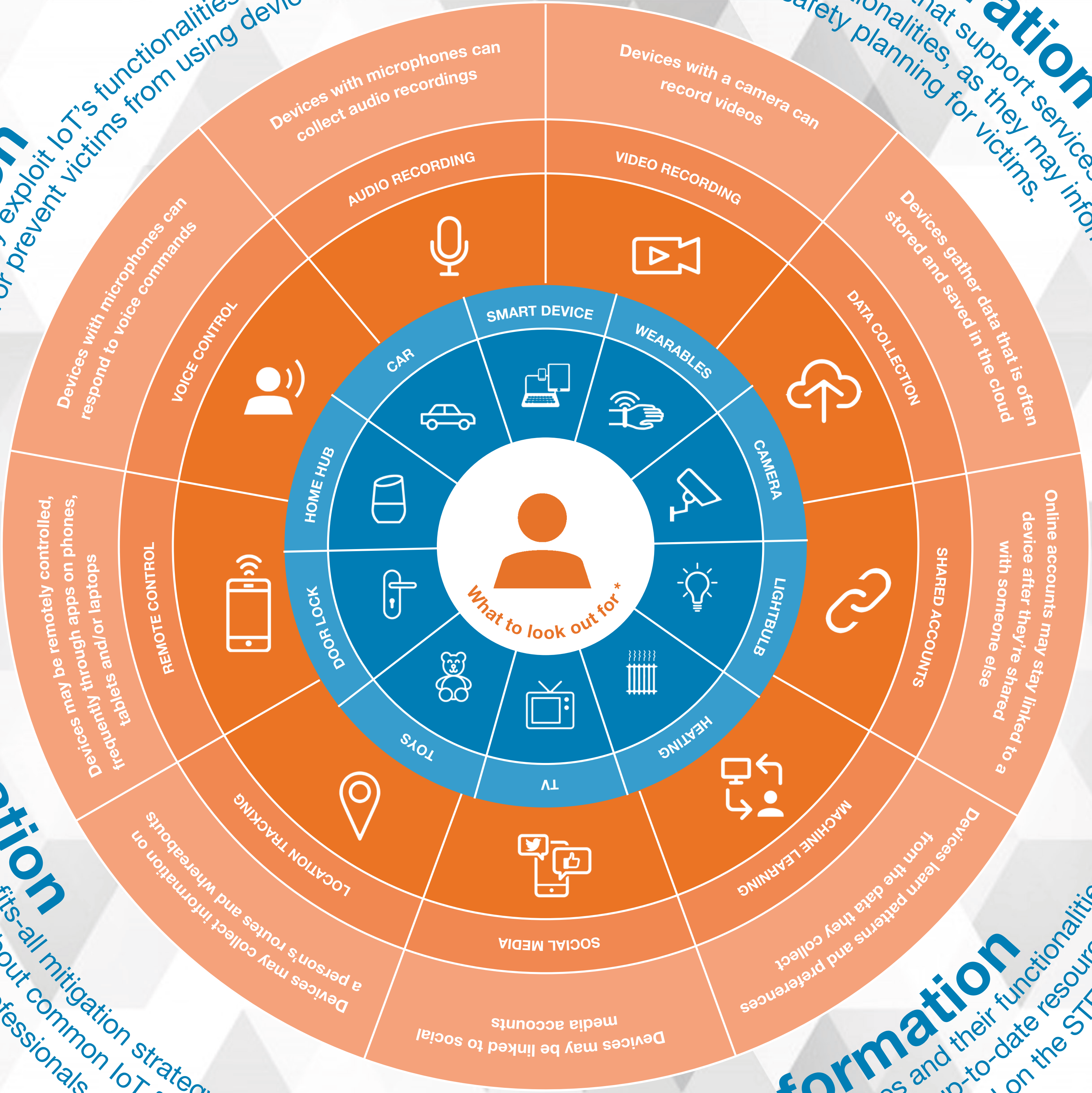
When IoT devices are connected to the internet they can communicate and share instructions with each other. This can result in privacy, security and safety risks, because devices assume all users trust each other. An abuser can potentially misuse the features of a device to monitor and control a victim. In the future, more of these devices may be part of public and private spaces.

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.



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 a person's routes and information on 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

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.

* This list is not exhaustive.

00.00

July 2018

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

PETRAS

London
VAWG
Consortium

PRIVACY
INTERNATIONAL

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