UCL
DEPARTMENT OF SCIENCE, TECHNOLOGY, ENGINEERING AND PUBLIC POLICY

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.

The growing risk of tech abuse

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. 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.[1]

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.

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 IoT devices' features to monitor and control a victim. In the future, more of these devices will be part of the public and private spaces.

1. IHS Markit. (2017). The Internet of Things: A movement, not a market. Englewood, United States: IHS Markit. Nordrum, A. (2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated. IEEE Spectrum

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.

Our research

This briefing was produced as part of the 'Gender and Internet of Things' project conducted by a research team based at UCL STEaPP and Computer Science. The study was funded by the UCL Social Science Plus+ scheme and the NEXTLEAP Project.
Research collaborators included the London VAWG Consortium, Privacy International and the PETRAS IoT Research Hub.

Additional resources

For support service providers
Gender and IoT Resource List
Gender and IoT Guide
Gender and IoT Newsletter

Further Information

Visit the project webpage:
https://www.ucl.ac.uk/steapp

Contact us

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

UCL Public Policy · London VAWG Consortium · PRIVACY INTERNATIONAL · PETRAS · NEXTLEAP · UCL COLLABORATIVE SOCIAL SCIENCE DOMAIN