TECH ABUSE

Gender and the Internet of Things ('IoT')
Futureproofing Online Harms legislation

The number of internet-connected devices is growing rapidly. One estimate[1] suggests there will be 500 billion internet-connected devices by 2030. The IoT is the network of these connected devices.

The IoT provides benefits for modern life, but it also creates opportunities for new types of harm. Perpetrators of domestic abuse can misuse IoT devices' features to monitor and control their victims. For example, internet-connected video cameras (such as on 'smart' doorbells) or wearable watches with integrated GPS tracking technology can allow victims to be spied upon by perpetrators. **The IoT enables three new types of crime that should be within scope of new Online Harms Legislation:**

a) Cyber stalking

Harassment taking place on or via the internet.

b) Coercive and controlling behaviour using IoT

Acts of abuse to harm, threaten or frighten a victim. This could involve the denying access to controls for heating, lighting, locks and security systems.

c) Digital gaslighting

A form of psychological abuse designed to make someone doubt their version of reality, for example by remotely operating smart building controls.

The Online Harms White Paper recognises the increased potential for cyber stalking, but it does not take account of how coercive and controlling behaviour or gaslighting could be undertaken using the IoT.

Government policy should incorporate these new types of online harms associated with internet-connected devices. We suggest three ways in which such harms could be incorporated into new policy and contribute to achieving the Government's ambition to 'make the UK the safest place to be online.'

1. **Introduce a new statutory duty of care on tech companies.**
2. **Provide guidance on tech abuse as part of the media literacy strategy.**
3. **Report and publish tech abuse data.**

[1]Cisco, 2016. Internet of Things. Available at: https://www.cisco.com/c/dam/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf

[2] DCMS, 2019. Online Harms White Paper. Available at : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

[3] eSafety Commissioner, 2019. Helping Australian's to have safer, more positive experiences online. Available at: https://www.esafety.gov.au/

1. Introduce a new statutory duty of care on tech companies

The regulatory framework of the Online Harms Bill should include a new statutory duty of care on technology companies to keep their users safe from digital gaslighting and coercive and controlling behaviour. These steps could include the following:

- **Dedicated services and means to report incidents** of harassment, including offline options (such as a phone number).
- Easy-to-use **tools that allow users to take control over the privacy** and offer visibility of their account settings (such as who can and has had access to it).
- **UK-wide recording practices** of technology-facilitated abuse forms, to keep abreast of the changing threat landscape.

2. Provide guidance on tech abuse

The media literacy strategy, part of the Government package to tackle online harms, should include a commitment to provide accessible up-to-date advice and guidance tailored to people at risk of tech abuse. This would be in scope of its aim to 'provide a coordinated and strategic approach to online media literacy education for children, young people and adults.' [2] The approach could be modelled on that of Australia, which has an 'eSafety Commissioner' to lead and coordinate online safety efforts.[3]

3. Report and publish tech abuse data

Nationwide data on tech abuse is not currently available. This makes it difficult for central and local Governments, the support sector and researchers to understand and monitor the scale and nature of the problem. Data on tech abuse needs to be collected and made available publicly in the **annual crime survey**. This could also allow the regulator to monitor companies whose systems are involved in domestic abuse cases.

For more information, contact:
Dr Leonie Tanczer, Principal Investigator
UCL Department of Science, Technology, Engineering and Public Policy (UCL STEaPP)
l.tanczer@ucl.ac.uk

Visit our website:
https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot

February 2020