Written response to the House of Commons DCMS Committee Inquiry "Connected Tech: Smart or Sinister?"

UCL Gender and Internet of Things (IoT) Research Project

June 2022

"Gender and IoT" (G-IoT) is an interdisciplinary research project at UCL. Our team analyses the evolving privacy and security risks of IoT systems in the context of domestic violence and abuse. We are pleased to respond to the Committee's inquiry on this important topic. Our response focuses on the specific risks to victims/survivors of domestic abuse from smart and connected technologies and what measures will be needed to mitigate against those risks.

This response has been prepared by Dr Leonie Tanczer, Lecturer in International Security and Emerging Technologies, with coordination from Florence Greatrix, Policy Adviser.

What has been or will be the most important impacts of increasingly prevalent smart and connected technology in our lives, including in the home, in the workplace and in our towns and cities, and are they necessarily better than current systems?

Abuse conducted through smart, internet-connected systems sits within and overlaps with different categories of abuse - such as harassment or coercion and control. The risks that IoT technologies generate are not necessarily unique, but they can broaden and exacerbate patterns of abuse, offering new ways for perpetrators to cause harm. We use the term "tech-abuse" to describe this type of abuse. This term has recently been adopted in various official Government documents, including the 2022 National Cyber Strategy,[1] and the Home Office draft (for consultation) Statutory Guidance Framework on Controlling and Coercive behaviour.[2]

We explain several examples of impacts of smart and connected technologies in the home below. We have previously highlighted these issues in our UCL/PETRAS report for DCMS on Consumer IoT security.[3]

Remote control

The person controlling the technology no longer needs to be physically present at their home to change the material environment, such as the heating or lighting system. In the context of domestic abuse, this allows perpetrators to adjust settings of devices from a distance using their phone and use this to "gaslight" their victims.

[1] UK National Cyber Strategy 2022. Available at: https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[2] Controlling or coercive behaviour statutory guidance consultation. Available at: https://www.gov.uk/government/consultations/controlling-or-coercive-behaviour-statutory-guidance

[3] The UK Code of practice for consumer IoT security: PETRAS UCL Research report 2022. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf

Automation
The automation of tasks such as timers on home heating systems is convenient. However, it could leave a victim/survivor of domestic abuse at risk if they do not have control of the system (for example, they do not have the correct password to log in and change the settings).

Inaccurate data profiles
The data collected by smart and connected technology forms profiles and records about their users, like their preferences and day-to-day behaviour. These might not always be complete or accurate for victims/survivors of domestic abuse. For example, they might have insurance behaviour or health profiles built up over a long period living with a perpetrator. The gathered data may not be an accurate representation of the victim/survivor, who might have been coerced and controlled during this period. How to rectify this inaccurate digital 'profile' is not yet clear.

Not understanding the capability of devices
IoT devices in the home have emerged recently and rapidly. As such, not everyone understands how to use them and their capabilities, particularly if someone else in their household purchased them or set them up. Domestic abuse perpetrators can use this to persuade or mislead their victim/survivor that their devices can perform certain activities, such as record video or audio, or access their personal device, when they cannot. Equally, perpetrators might be able to use compromised smart devices to monitor their victim/survivor without them realising, such as to find out when they enter or leave the house.

Are there any groups in society who may particularly benefit from or be vulnerable to the increasing prevalence of smart technology, such as young or elderly people, people with disabilities and people likely to be digitally excluded?

There are specific vulnerabilities for victims/survivors of domestic abuse that derive from smart, connected devices. The risks they generate are not necessarily new or unique. Rather, they can enable or facilitate domestic abuse, change patterns of abuse, and extend a perpetrator's 'reach'. Specifically, the functionalities that these devices and systems provide (such as those listed in our answer to the previous question) offer perpetrators a range of avenues to monitor and control victims/survivors.

How can we incentivise or encourage design that is safe, secure, environmentally- and user-friendly and human rights compliant?

Our research has found that a combination of guidelines, standards, and best practice along with regulatory/financial repercussions for manufacturers who do not abide by these guidelines is needed. The Consumer IoT Code of Practise (CoP)[4] and the forthcoming Product Security legislation[5] (which intends to mandate some of these principles) is a start but does not go far enough. We provide more detail in our response to the final question.

[4] Code of Practise for Consumer IoT security 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf

[5] Product security and telecommunications infrastructure Bill documents. Available at: https://www.gov.uk/government/publications/product-security-and-telecommunications-infrastructure-bill-documents

We suggest two further ideas for ways to incentivise or encourage the design for more secure IoT systems:

Gather data

We need National Crime Statistics to be updated and the databases analysed to identify the types of tech-abuse being reported and understand the scale of the problem. Ideally, we would then examine data gathered by support services to evaluate which digital systems (including social media and Internet-connected devices) are being used in domestic abuse cases or other criminal activity and how they are deployed and manipulated.

Diversify the market

Supporting a more heterogeneous IoT market (for example, through financial incentives and investment in universities) with more than the 'big players' would set standards for others to follow.

What are the key short- and long-term risks and threats, and how can we ensure the devices, systems and networks of individuals, businesses and organisations are digitally literate and cyber secure?

Short- and long-term risks and threats

The risk landscape for IoT devices is changing and evolving. Its cyber-physical nature means that risks can have both digital and physical implications, including surveillance and physical harm. Our response to the previous question provides some examples of this.

The standards, governance, and policy of consumer IoT will require constant reconsideration as their use (and misuse) evolves and changes. For example, regulations following the forthcoming Product Security and Telecommunications Infrastructure Bill need to have a broad scope to cover new devices or capabilities of devices that are not yet on the market.

Our 2018 UCL/PETRAS research report with Lloyds[6] goes into further detail on the changing risk landscape and short- and long-term risks in the context of domestic abuse.

Ensuring digital literacy and cyber security

The UK could take note of recent actions by the Australian Office of the eSafety Commissioner. This is a centralised public body that provides information, help and support for the Australian public about online risks and harms. For instance, the eSafety Office promotes online safety education for a variety of communities (including teachers, children, and parents). They remove inappropriate content found online, liaises with tech vendors to help mitigate risks, and conducts research and develops public-facing resources.[7]

Education on the risks posed by IoT devices is important. An idea we have previously suggested is deploying public figures to convey key messages. For example, a "David Attenborough of IoT" could become the face of IoT security and run documentaries and

[6] Networked world. Risks and opportunities in the Internet of Things. Available at: https://assets.lloyds.com/assets/pdf-networked-world-2018/1/pdf-networked-world-2018.pdf

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

information channels to reach a wide audience. This could convey the message to the UK audience in an understandable way without being perceived as alarmist.[8]

How will current geopolitical concerns influence domestic consumers, e.g., regarding standards of imported goods or in how we can deal with cyber threats?

The current centralisation of market powers (such as Google, Amazon, and Apple) means they have the backing, knowledge, and skills, combined with existing public reputation to dominate the IoT market – just like they did with smartphones, laptops, and tablets. We are concerned that key "nodes" in the IoT environment (such as the Google Home and Amazon Echo) could become 'gatekeepers' that set standards and requirements for others looking to enter the IoT market, given that smart speakers are often the central contact point amongst various connected devices in the home.

Ensuring diversity in market players and guaranteeing interoperability and data portability (explained further in our next answer) are essential for IoT security and for reducing the tech-abuse threat.

Do existing frameworks, like data protection legislation and the Public Security and Telecommunications Infrastructure Bill, adequately address concerns with smart technology, and if not, how could they be changed?

The Product Security and Telecommunications Infrastructure Bill will provide regulation-making powers for three principles from the 2018 CoP. The development of this voluntary CoP was a good example of a collaboration between academia and government, but it had a poor take up from industry, and so necessarily some principles are now being written into law. The Bill factsheet cites domestic abuse from these technologies as one reason for this legislation.[9]

The Bill suggests the Government is taking tech-abuse seriously after understanding the findings of our research and the work of domestic abuse charities such as Refuge. While the Bill has good intentions in making consumer IoT more secure, there is still more to be done. This could include mandating the other principles from the CoP.

The right to data portability, outlined in the EU General Data Protection Regulations (GDPR), allows 'data subjects' (individuals who can be identified or who is identifiable) to transfer their data from one service to another. However, our research has found that it is not possible to exercise this right with IoT devices.[10] If it were possible, this could help to increase the diversity of IoT devices on the market. Regulators and researchers need to trial and test existing legislation as we did here, to ensure the rights of individuals/consumers can be exercised.

[8] Governance and policy cooperation on the cybersecurity of the IoT 2018. Available at: https://discovery.ucl.ac.uk/id/eprint/10063234/1/Carr_Report_Global-governance-of-the-Internet-of-Things-Report-PDF.pdf

[9] Same as 8.

[10] Turner, S., Galindo Quintero, J., Turner, S., Lis, J. and Tanczer, L.M., 2021. The exercisability of the right to data portability in the emerging Internet of Things (IoT) environment. *new media & society*, *23*(10), pp.2861-2881. Available at: https://discovery.ucl.ac.uk/id/eprint/10104741/14/Tanczer_1461444820934033.pdf