Written evidence submitted by the
'Gender and Internet of Things' Research Team
University College London (UCL)

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

Introduction

We welcome the opportunity to contribute to the Committee's inquiry. Our evidence is based on recent research we have conducted into how the Internet of Things (IoT) might impact on gender-based domestic violence and abuse and what measures will be needed in order to mitigate against those risks.

We see the growth of 'smart', internet-connected devices (such as voice-activated home hubs, smart central heating and smart security systems) as creating a new risk, where these technologies serve to exacerbate the ability of perpetrators of domestic abuse to manipulate and dominate victims. We believe that it is important that the forthcoming draft Domestic Abuse Bill is 'future proofed' against these risks.

We believe the following measures are necessary to mitigate this emerging risk:

- Acknowledging the existence of this emerging risk through including a specific reference to 'tech abuse' in the definition of domestic abuse.
- Improving technical expertise for front-line support workers.
- Including tech-abuse as a factor in risk assessment and safety planning of victims.
- Expanding the focus of tech-abuse to include emerging technologies such as the Internet of Things.
- Creating tech-abuse guidance for support services.
- Regulating the prevalence of spyware in consumer products.
- Collecting data on technology-facilitated abuse in order to better understand the extent of this phenomenon and the demographics of victims and perpetrators. (This information is not routinely collected at present.)

Below we address the specific terms of reference of the Committee's inquiry.

What further measures need to be taken to help prevent domestic abuse

We believe that further action is needed to respond to new threats arising from emerging 'smart' internet-connected devices (such as voice-activated home hubs, smart central heating and lighting systems and smart security systems).

In recent years, forms of online harassment and sexual abuse facilitated through information and communication technologies (ICT) have emerged. These ICT-supported assaults range from cyber stalking to online behavioural control.

Although efforts concerned with 'conventional' cyber risks (such as abuses on social media platforms and restrictions to devices such as laptops and phones) have been set in place, we expect that new forms of technology-facilitated abuse, so-called 'tech-abuse' will appear.

In particular, we anticipate a rise in internet-enabled technologies through the use of 'smart' devices, which are frequently disguised in terms of their ability to sense accentuate, and collect private data. These 'Internet of Things' (IoT) systems offer

unique and potentially unforeseen means to *exacerbate* perpetrators' ability to manipulate and dominate (for example, remote control of heating, lights, locks), as highlighted most recently in instances where a husband used a smart-home device to spy on his wife.[1] Or where the internet-enabled 'Amazon Alexa' recorded and sent private audio information to a random person in a user's contact list.[2]

While IoT usage is not yet widespread (7.5bn total connections worldwide in 2017), it is expected to increase to 25.1bn connections globally by 2025.[3] This expansion together with society's growing digitisation should consequently be on the radar of legislators who hope to prepare for these societal and technical changes.

In order to ensure that the UK's legislation in this area is 'future proofed', we recommend that the definition of domestic abuse should include an explicit reference to tech-abuse, as follows:

> "Any incident or pattern of incidents of controlling, coercive, threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexual orientation. The abuse can encompass, but is not limited to: psychological, physical, sexual, economic, emotional, *and technological*."
>
> "Controlling behaviour is a range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating *as well as monitoring* their everyday behaviour."

Including a specific reference to technology-facilitated abuse and its monitoring features would increase the level of awareness of this emerging new risk and should help to keep victims safe both off- and online.

Is the response of public authorities to domestic abuse good enough, and if not, how could it be improved?

1. Improving technical expertise for front-line support workers

Our study involved in-depth interviews and workshops with representatives of voluntary and statutory domestic violence and abuse support services as well as academics. We uncovered pressing evidence of the need for more support in the area of tech-abuse. A wide-spread problem raised by respondents of the voluntary and statutory domestic violence and abuse sector included the lack of expertise by support services that encounter tech-abuse victims.

One of our interview respondents from the charitable sector described why there is a greater need for such specialist knowledge and corresponding technical capabilities:

[1] The Times (2018). Husband used smart-home device to spy on wife.
[2] BBC (2018). Amazon Alexa heard and sent private chat.
[3] GSMA (2018). The Mobile Economy Report.

> "I would like them [victims] to have somewhere that they could go to where […] the person they're sitting with (a) understands abuse and understands the impact of have had your email hacked or your whereabouts monitored, or your social media gone into . […] But, secondly, I'd like that person to be able to go into her devices or her mobile or her tablet and extract evidence that is unquestionable so that the police will begin to make prosecutions and, and we will begin to have successful prosecutions and convictions."

We therefore encourage the UK government to prioritise tech abuse as a funding area across the whole sector.

We note that there are some examples of statutory services beginning to recognise the need for additional capacity in this area. For example, the Northumbria Police has recently increased its technical capabilities, including establishing a dedicated domestic abuse cyber stalking and harassment team. Approaches like this have to become more widespread to ensure the availability of know-how and specialist help across the UK. The existence of such teams also needs to be effectively communicated to refuges, charitable organisations and frontline workers.

2. Ensuring there is an appropriate gender balance in police units dealing with technology

An observation that derived from our engagement and interactions with statutory and charitable support services is the perceived lack of female officers in the UK police force, especially in units that deal with technology. There is a body of literature emphasising female rape and sexual assault victims' preference for dealing with female police officers and the positive effects that female police representatives can have on the response and arrest rates when it comes to gender-based sexual violence.[4]

While our research team has currently no hard evidence to verify nor to make judgements on the effects of such a potential gender-imbalance, we do suggest it would be it would be helpful to review the gender-balance of staffing in areas of domestic violence and tech-abuse.

[4] Andrews, R., & Miller, K. J. (2013). Representative Bureaucracy, Gender, and Policing: The Case of Domestic Violence Arrests in England. Public Administration, 91(4), 998–1014.
Jordan, J. (2002). Will any woman do?: Police, gender and rape victims. Policing: An International Journal, 25(2), 319–344.
Meier, K. J., & Nicholson-Crotty, J. (2006). Gender, Representative Bureaucracy, and Law Enforcement: The Case of Sexual Assault. Public Administration Review, 66(6), 850–860.

What else is required to ensure that there is sufficient support, protection and refuge for victims of abuse?

We propose the following actions that derive from our ongoing research on the implications of the IoT on gender-based domestic violence and abuse.

1. **Including tech-abuse as a factor in the risk assessment of victims**

The standardised SafeLives Dash risk checklist[5] is being used across the sector (including statuary and charitable support services) and facilitates the first contact with victims of domestic violence and abuse. However, technology-facilitated abuse it currently not explicitly addressed in the document. Many respondents (including frontline workers) have referred to the need to review and update the checklist and expressed that tech-abuse may be "something SafeLives need to consider" and that "implementing an aspect for tech [-abuse] would be really useful".

We are aware that the College of Policing is at the moment reviewing the SafeLives Dash risk checklist. This offers an opportunity to propose respective amendments.

2. **Include tech-abuse as a factor in the safety planning of victims**

Based on our research, we consider it necessary to review safety planning policies by support services, which also requires amendments to current guidance and training. These policies should focus not only on victim's physical safety, but also their digital security when it comes to their Internet usage and the security of their phone, tablets and increasingly emerging technologies such as IoT systems (e.g., 'smart' locks, energy and heating meters, toys and other household appliances).

3. **Expand the focus on tech-abuse to emerging technologies such as the Internet of Things**

Our research and the engagement with charitable and statutory support services has revealed that the actions set in place to support victims of tech-abuse are often too narrowly focused on phones, laptops, satnavs, apps, and social media platforms.

The G-IoT research project looks specifically at emerging technologies such as 'smart' devices and systems, which include Internet-connected objects commonly used in the household. We propose that tech-abuse trainings and guidance should account for these technological changes and the risk trajectories that Internet-enabled devices bring (for example, remote control of systems, their tracking/location capability, as well as their audio and video functionality).

4. **Create tech-abuse guidance and increase expertise**

Interviewees and focus group participants have highlighted that support services' knowledge base is their "biggest challenge" when it comes to tech-abuse. Many respondents expressed that they "don't know what [technical] advice and information

[5] SafeLives (2015). Dash risk checklist: Quick start guidance.

to give to women" or who to contact when they suspect technical interference or tampering.

To address this gap, we consider it essential that the UK government ensures that there is dynamic guidance set in place where frontline workers, support services as well as victims can keep themselves informed about the functionality, risks and opportunities that technologies such as apps but also IoT systems create. The material should be easy to use and applicable to different devices and service needs. Such resources may go hand in hand with ongoing advice produced by 'Cyber Aware' or the National Cyber Security Centre (NCSC) which may be able to provide assistance for domestic violence and abuse victims.

An example of a similar initiative is the 'eSafety Women' website which is an online service produced by the Australian Government. It uses interactive infographics to help familiarise victims as well as the general public with devices that may be a threat within the home or the car.[6]

Additionally, to address support services' "lack of knowledge on the cyber side", dedicated tech-abuse trainings as well as tech-abuse teams for support services may be set in place. These trainings and teams can help communicate the developed guidance and provide, for example, frontline workers with the knowledge and awareness to support and direct victims of tech-abuse. Refuge is at the forefront in this regard and has set in place a new programme which was funded by Google.org. The programme is aimed at protecting women from tech abuse and meant to empower them to use technology safely.

5. Reduce/remove prevalence of spyware

Across our research, respondents have consistently referred to the prevalence of spy software, so-called spyware - such as iPhone's 'Find My Phone' app, 'Spyzie' or 'FlexiSPY'. Many of these services are often explicitly advertised to allow the tracking of partners or are repurposed when promoted as being useful to monitor children or employees.

Most recently, Chatterjee et al. (2018) assessed the full extent of these spyware systems and offered the first in-depth study of the intimate partner spyware ecosystem.[7] The authors found that the majority of software solutions are 'dual-use' apps in that they have a legitimate purpose (e.g., child safety or anti-theft), but are easily and effectively repurposed for spying on a partner. Chatterjee et al. (2018) document that a wealth of online resources available to educate abusers about these exploiting apps and uncover the dedicated advertisements, blogs, and customer support services that have been set in place.

Aligned with the research conducted by Chatterjee et al. (2018) and the findings from our own study, we suggest that the UK Government should closely examine this

[6] eSafetyWomen (2018). Take the Tour.
[7] Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., … Ristenpart, T. (n.d.). The Spyware Used in Intimate Partner Violence. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 993–1010).

market and consider both technological as well as legal and regulatory means to prevent the misuse of such tools.

What national oversight framework is required to ensure that there are sufficient quality services available at a local level for victims of abuse?

There is currently no consistent collection and assessment of technology-facilitated abuse information. We think it is important to compile this data to:

1. provide an overview of the full scope and extent of tech-abuse;
2. begin a longitudinal analysis of the patterns, changes, and dynamics of tech-abuse; and
3. generate information about the demographics of common tech-abuse victims and perpetrators.

As a response to our research, various charitable support services expressed that they are planning to “stress test” and “add technology” to their assessment stage and aim to “measures” and “catalogue[e]” incidents and their prevalence.

Similarly, the ONS ‘Domestic abuse in England and Wales’ dataset and statutory as well as voluntary services should be incentivised to trace tech-abuse in their assessments, questionnaires and surveys.

About our research

I am answering this call in my role as Principal Investigator for the ongoing 'Gender and Internet of Things' (G-IoT) research project.[8] G-IoT is an interdisciplinary study exploring the implications of Internet of Things (IoT) on gender-based domestic violence and abuse. It is funded by a Social Science Plus+ award from UCL's Collaborative Social Science Domain.

The project team involves myself, Dr Trupti Patel, Dr Simon Parkin, and Professor George Danezis and is run in collaboration with the London Violence Against Women and Girls (VAWG) Consortium, Privacy International, and the PETRAS Internet of Things Research Hub. I am responding to this Consultation in a representative function and wish to solely speak for the academic research team at UCL.

Our submission is based on ongoing research conducted in 2018. Our study involved to this point 4 in-depth interviews and 2 workshops in the course of which we run focus groups with around 45 individuals. The latter were representatives of voluntary and statutory domestic violence and abuse support services as well as academics.

Our research team has developed information material for support services, including a guide[9] as well as a resource list[10], which has been featured amongst others, in the BBC[11], WIRED UK[12], and the Engineering and Technology Magazine[13].

Dr Leonie Maria Tanczer
Research Associate (PETRAS IoT Hub)
Department of Science, Technology, Engineering and Public Policy (STEaPP)
University College London

July 2018

[8] Tanczer, L., Parkin, S., Patel, T., & Danezis, G. (2018). Gender and IoT.
[9] Tanczer, L., Parkin, S., Patel, T., & Danezis, G. (2018). G-IoT guide
[10] Tanczer, L., Parkin, S., Patel, T., & Danezis, G. (2018). G-IoT resource list
[11] BBC News. (2018, July 9). Smart home gadgets domestic abuse warning. *BBC News*. Retrieved from https://www.bbc.com/news/technology-44765830
[12] Braithwaite, P. (2018, July 22). Smart home tech is being turned into a tool for domestic abuse. *Wired UK*. Retrieved from https://www.wired.co.uk/article/internet-of-things-smart-home-domestic-abuse
[13] Vella, H. (2018, June 20). IoT devices and smart domestic abuse: who has the controls? Retrieved June 29, 2018, from https://eandt.theiet.org/content/articles/2018/06/iot-devices-and-smart-domestic-abuse-who-has-the-controls/