“Transforming the Response to Domestic Abuse” Government Consultation

May 2018

Response by the “Gender and IoT” Research Team

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

Personal Details

A. I understand that there are two versions of the consultation. If I have already completed the short version I will not answer the following questions again: 6, 7, 9, 12, 24, 25, 26, 32, 35, 39, 43.

Yes

B. What is your name?

Dr Leonie Maria Tanczer

C. What is your email address?

l.tanczer@ucl.ac.uk

D. What region are you in?

Greater London

E. Are you responding on behalf of an organisation or as a member of the public?

Organisation

F. If relevant, which, if any, best describes you/your organisation?

Researcher

G. If applicable, please give the name of your organisation/ profession.

University College London (UCL), Department of Science, Technology, Engineering and Public Policy (STEaPP)

I am answering this call in my role as Principal Investigator for the ongoing 'Gender and Internet of Things' (G-IoT) research project. 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 (https://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/dpl-projects/gender-and-iot).

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 (https://thelondonvawgconsortium.org.uk/), Privacy International (https://privacyinternational.org/), and the PETRAS Internet of Things Research Hub (https://www.petrashub.org/). 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.

Introducing a new statutory definition of domestic abuse

1. Do you agree with the proposed approach to the statutory definition?

Strongly Agree

Please explain your answer.
While our research supports the broader definition of domestic abuse, we would also like to see an explicit recognition of the role that technology can play in facilitating and exacerbating abuse included in the definition.

Technology is not only a means to potentially tackle domestic abuse (for example, e-monitoring), but more profoundly a means to facilitate psychological, physical, sexual, economic, and emotional abuse as well as controlling and coercive behaviour.

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 such 'conventional' cyber risks (for example, 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 (The Times, 2018) or where the Internet-enabled 'Amazon Alexa' recorded and sent private audio information to a random person in a user's contact list (BBC, 2018).

While IoT usage is not yet widespread (7.5bn total connections worldwide in 2017), it is expected to internationally increase to 25.1bn connections globally by 2025 (GSMA, 2018). 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.

We propose that the definition should be amended to read:

"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 on this emerging risk vector and should help to keep victims safe both off- and online.

References:

BBC (2018). Amazon Alexa heard and sent private chat. http://www.bbc.co.uk/news/technology-44248122

GSMA (2018). The Mobile Economy Report. https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/05/The-Mobile-Economy-2018.pdf

The Times (2018). Husband used smart-home device to spy on wife. https://www.thetimes.co.uk/article/husband-used-smart-home-device-to-spy-on-wife-3xzcfqp3m

Improving support services for all victims of domestic abuse and their children

10. We are in the process of identifying priority areas for central Government funding on domestic abuse. Which of the following areas do you think the UK Government should prioritise? Please select up to 3.

X Advocacy for victims to enable them to stay safely in their own home (Independent Domestic Violence Advisors or their equivalent)
X Therapeutic services to help victims of domestic recover from their experience
X Accommodation services
X Helpline services for those affected by domestic abuse to call for advice and support
X Interventions embedded in health
X Perpetrator programmes which aim to change offenders' behaviour and stop reoffending
X Rolling out of new multi-agency approaches
• Don't know/no answer
X Other - please explain

If you selected other please add your response here

Our research team supports the funding of all of the above-mentioned areas. However, based on our current study, we find pressing evidence 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 support sector described why there is a greater need for such specialist knowledge and corresponding technical capabilities: “I would like them [victims] to have somewhere that they could go to where, um, the person they're sitting with a) understands abuse and understands the impact of having 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, thus, encourage the UK Government to prioritise tech abuse as a funding area across the whole sector. An example of a statutory service which has recently increased its technical capabilities includes the dedicated domestic abuse cyber stalking and harassment team established within the Northumbria Police.

Such developments have to become more widespread to ensure the availability of know-how and specialist help across the UK and demand for a multi-agency response

that is fit for purpose as ‘smart’ devices become more prevalent. The existence of such teams needs to be also effectively communicated with refuges, charitable organisations, and frontline workers.

Online threats and the role of technology in domestic abuse

36. What more can we do to tackle domestic abuse which is perpetrated online, or through control of technology?

- X Appropriate reporting categories on social media platforms and signposting victims to off-platform support, such as helplines
- X Clear guidance from social media companies on privacy settings for users at risk or victims of domestic abuse on online domestic abuse
- X Effective use and handling of evidence from social media within the investigation and prosecution processes
- X Government / charities and others promoting awareness of online and technology risks in relation to domestic abuse, such as through advertising
- X Government raising awareness of the use of spyware or GPS locators on phone or computers by perpetrators
- X Retailers, applications and the wider technology industry raising awareness of the use of spyware or GPS locators on phone or computers by perpetrators
- Don't know/no answer
- X Other - please explain

Use this box to explain your answer or if you selected 'other'

Our research team supports the above-mentioned measures but would like to propose additional actions that derive from our ongoing research on the implications of the IoT on gender-based domestic violence and abuse. These include, but are certainly not limited to the following aspects:

(1) Tech-abuse as a factor in the risk assessment of victims;

The standardised SafeLives Dash risk checklist (http://safelives.org.uk/sites/default/files/resources/Dash%20for%20IDVAs%20FINAL.pdf) 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) Tech-abuse as a factor in the safety planning of victims;

Based on our research, we consider it of importance 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;

Touching on Point 2, 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 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 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 help 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: https://www.esafety.gov.au/women/take-the-tour#/

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

Reference:
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). https://doi.org/10.1109/SP.2018.00061

Improving the police response

37. How can we continue to encourage and support improvements in the policing response to domestic abuse across all forces and improve outcomes for victims?

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 (Jordan, 2002) and the positive effects that female police representatives can have on the response and arrest rates when it comes to gender-based sexual violence (Andrews and Miller, 2013; Meier and Nicholson-Crotty, 2006).

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 the UK Government to assess its police staffing in areas of domestic violence and tech-abuse.

References:

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. https://doi.org/10.1111/padm.12002

Jordan, J. (2002). Will any woman do?: Police, gender and rape victims. *Policing: An International Journal*, *25*(2), 319–344. https://doi.org/10.1108/13639510210429392

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. https://doi.org/10.1111/j.1540-6210.2006.00653.x

Improving performance using data

58. Please select which of the following you believe should be priorities for improving data collection. Please choose up to 3.

- X Improving the collection and reporting of data on when domestic abuse is a feature of a case/ intervention
- X Improving collection and reporting of data relating to the gender and relationship of the perpetrator and victim
- X Improving data to enable better tracking of outcomes in domestic abuse cases/ intervention
- Linking data to enable better tracking of interventions and reoffending
- Linking data to enable better understanding of the interactions/relationships between domestic abuse and other types of offending
- None of the above
- Don't know/ No answer
- Other - please explain

Please explain.

Our research supports that there is currently no consistent collection and assessment of technology-facilitated abuse information. We think it is important to compile this data to a) provide an overview of the full scope and extent of tech-abuse; b) begin a longitudinal analysis of the patterns, changes, and dynamics of tech-abuse; c) 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 more” and “add technology” to their assessment stage and aim to “measure” and “catalogu[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.