Written Submission to the Online Harms White Paper Consultation

UCL's Gender and Internet of Things (IoT) Research Project

June 2019

Introduction

The "Gender and Internet of Things" (GIoT) research team at UCL investigates the growing risk of technology-facilitated abuse in the context of domestic and sexual violence, hereafter termed "tech abuse". We are particularly studying the effect of smart, Internet-connected devices (so-called "Internet of Things; IoT) on victims/survivors of domestic and sexual abuse. We have previously responded to the UK Government's "Transforming the Response to Domestic Abuse" consultation [1] and are delighted to offer pre-legislative scrutiny also of this policy document. Our written evidence concerns the absence of the recognition of IoT-facilitated tech abuse in the Online Harms White Paper.

Key Points

- The remit of online harms should **not be restricted to social media platforms** but account for the growing risks derived from cyber-physical systems such as Internet-connected household devices or wearables. These systems present new channels for domestic abuse activities, including stalking and intimidating and controlling victims in their own homes.
- **IoT-facilitated tech abuse**, especially in the context of domestic and sexual violence, should be explicitly referenced in the Online Harms White Paper to enable public recognition of this form of abuse and future-proof UK law to protect victims/survivors against this form of abuse.
- The UK Government can foster a culture of transparency and accountability by making the transparency report's underpinning data should be made **publicly available** and by establishing a **centralised helpline** for support services working with victims/survivors of tech abuse.
- The risk derived from **"stalkerware" or "spouseware"**, which describes application that can be installed on phones and other systems such as laptops to – often secretly – monitor employees, children but increasingly also partners should be tackled in the Online Harms White Paper.
- Organisations need **practical guidance to build products which are secure by design** for minimising the risks of tech-abuse, including: offering user friendly methods for reviewing history and logs, offer users prompts and notifications, and designing intimate threat models.

Question 1: This government has committed to **annual transparency reporting**. Beyond the measures set out in this White Paper, should the government do more to build a culture of transparency, trust and accountability across industry and, if so, what?

We welcome the proposal to implement a regulator who will have the power to require annual reports from companies. To help build a culture of transparency, trust and accountability across industry, we propose three possible measures:

1. **Recognise technology-facilitated forms of intimate partner violence**

The regulatory framework as proposed will require companies to outline "the prevalence of harmful content on their platforms and what measures they are taking to address this" (Section 3.18, page 44). We hope that the reporting obligation as well as the draft transparency reporting template will give explicit recognition to forms of intimate partner violence. Companies could in this instance be expected to indicate the number and nature of domestic and sexual violence reports received and the actions implemented to tackle such requests.

2. **Make reporting data publicly available**

As researchers at one of UK's leading research institutions, we would welcome a decision to make the transparency report's underpinning data publicly available. This would relieve the current lack of tech abuse data accessible to scholars [2] and could enable researchers, charities, and other civil society organisations to use this data for further analysis. It would also open up opportunities for international exchange and comparison.

3. **Create customer-facing staff guidance**

For the tech sector to build a culture of transparency, trust, and accountability, the GIoT team hopes companies will create customer-facing staff guidance to implement appropriate referral and escalation procedures for victims/survivors of tech abuse. A useful example is the recent industry guideline "G660:2018 Assisting Customers Experiencing Domestic and Family Violence" by the Australian Communications Alliance Ltd [3]. The document is written for the telecommunication sector and outlines the many forms domestic and family violence can take.

The guidance includes examples of signs customers may express when under the influence of violence, coercion, and control, and steps telecommunication providers can take to mitigate possible risks for victims/survivors. It also contains information, tools, options and examples of good practices for providers to choose from. Similar documents for other tech sectors could be beneficial. Any experiences generated from the implementation of the guidance could further feature in the annual transparency report.

Question 3: What, if any, **other measures** should the government consider for users who wish to raise concerns about specific pieces of harmful content or activity, and/or breaches of the duty of care?

We suggest four possible measures the UK Government should consider:

1. **Expand the remit of online harms to account for the growing risks of technology-facilitated domestic and sexual violence.**

The Online Harms White Paper addresses harassment and comments on the gendered dimension of online harms (Section 7.21, Page 69). Yet, there is not an explicit acknowledgement of the harms caused by potential misuse of technology in the context intimate partner situations such as domestic abuse. Research shows the widespread use of technology in these instances [4]–[8]. For example, Internet-connected devices such as smartphones are used to track people's whereabouts and Internet-enabled lighting, heating, and security systems have been misused to intimidate and control. We, thus hope to see a tailored recognition and a dedicated set of measures for users suffering from technology-facilitated forms of domestic and sexual violence and abuse.

2. **Expand the remit of online harms to account for the growing risks derived from cyber-physical systems such as Internet-connected household devices or wearables.**

We note that the Online Harms White Paper as a whole is overly focused on social media. While the White Paper briefly comments on IoT (Box 32, Page 83), we would like to see future legislation covering not only platforms but also emerging technologies such as 'smart' Internet-connected devices. These IoT systems offer unique and potentially unforeseen means to exacerbate perpetrators ability to manipulate and dominate (for example, remote control of heating, lights, locks).

This has been clearly shown by our research team [2], [9], [10] and other studies [11], [12], echoes domestic abuse support services concerns [13]–[15] as well as recent media reporting where IoT systems featured in tech abuse cases [16]–[18]. 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 [19]. Thus, to "future proof" this legislation, reference to these novel forms of cyber-physical harms should not be ignored.

3. **Recognise the use of malicious software, so-called "Spyware" or "Spouseware".**

Similar to the risks associated with smart, Internet-connected devices, the threat of spyware has not been addressed in the Online Harms White Paper. Across our research, respondents have consistently referred to the prevalence of spy software, so-called

spyware - such as ‘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. Research by Chatterjee et al. [20] 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. Based on the current state of evidence, we therefore suggest that the UK Government should closely examines this market and consider both technological as well as legal and regulatory means to prevent the harms deriving from these tools.

4. **Offer a centralised helpline for support services to raise concerns about specific pieces of harmful content, breaches of the duty of care, and IoT-facilitated tech abuse.**

Our engagement with domestic abuse support services has shown that both statutory and voluntary organisations face shortcomings in responding to technology-facilitated domestic and sexual violence and abuse [2]. In order to tackle the support sector’s challenges with tech abuse, we would like to see the development of a centralised helpline to support services who may not have the knowledge or capacity to respond to different tech abuse risk vectors. Similar to developments happening in Luxemburg and Slovakia, where bodies such as the National Computer Security Incident Response Team (CIRCL, CERT SI) provide guidance for domestic violence services and tech abuse victims/survivors [21], [22]. The GIoT team has previously put forward to idea of having the National Cyber Security Centre (NCSC) providing a similar offering in the UK [2].

Question 16: What, if any, are the most significant areas in which organisations need **practical guidance** to build products that are safe by design?

Our research has found a number of areas which require organisations to receive guidance to build products that are safe by design. These suggestions extent the current “UK Code of Practice for Consumer IoT Devices” and other secure by design as well as data protection by design principles [23]:

1. **Improve internet router security and usability**

There is a need for practical guidance on Internet router security and usability, which will benefit the average user as much as vulnerable groups such as domestic violence victims/survivors. Internet routers effectively act as gateway for the smart, Internet-connected home and are, thus, of central criticality. While conventional Internet routers enable users to change passwords or generate separate networks with distinct log-in credentials (e.g., a “public network” for guests versus a “private network” for residents and their devices), many routers are not user-friendly enough for the average consumers to

make use of these features [24]. Besides, we suspect there is not enough awareness of the level of importance of this functionality. However, as society moves into an increasingly interconnected IoT environment, the reduction of cyber-physical harms will also be dependent on the level of security offered by these essential gateways. Increased user-friendly settings will provide victims/survivors with easier means to control the amount of devices connected to their network.

2. **Offer user-friendly methods to review history and logs**

In line with a need for better Internet router security and usability, the GIoT team considers it essential for users to easily review search requests and connectivity logs (e.g., which devices/accounts/IP addresses have recently connected to my system). These review options may take the form of services offering an easily accessible page where users can review "who has connected to what, when" or may be linked with the earlier discussed improvements to the usability of Internet routers. The UK Government consequently may choose to encourage app developers as well as IoT manufacturers to make it as simple as possible for users to verify their extent and level of connectivity. This way, unknown apps or IoT systems that are coupled to one's network or device can be easily removed. The feature would be particularly helpful for malicious software such as spyware.

3. **Offer prompts and notifications**

Users frequently switch on features that leave them, for example, susceptible to location tracking. Our research suggests it is important for users to receive regular, pro-active prompts and notifications on the extent of apps or IoT devices being in usage at a given set of time [2], [9]. In addition, prompts and notifications can provide a mechanism for users as much as domestic and sexual violence victims/survivors to be reminded to block or switch of features such as location tracking at times of non-usage.

4. **Design intimate threat models**

For truly 'safe by design' products, organisations need to incorporate the threat of intimate partner violence as well as coercion and control at each stage of the product lifecycle. This could include incorporating intimate partner violence in threat assessments or threat modelling, usability testing, and security testing. Existing work suggests that security analysis of smart home devices tends to consider "external" threats, such as remote network based adversaries or thieves [10]. Yet, threat models should also include perpetrators who are close to and may live with the victim/survivor. This could include a partner, family members or other flatmates. Such considerations should influence technological design and tools for victims/survivors to keep using technology safely. These models should be applied not only to conventional platforms (phone apps, social media) but also to emerging technologies such as IoT systems. The intimate treat model should extend into the product support stage, so that companies have procedures for addressing reported cases of IoT abuse (see response to Question 1: Customer-facing staff guidance).

Question 17: Should the government be doing more to **help people manage** their own and their children's online safety and, if so, what?

In terms of the education and awareness on safety and security (also raised in Question 18 of this Consultation), we would like to see the regulator have a role in at least the following three areas:

1. **Acknowledgment of the accumulated risks deriving from the infringement of children's privacy in the context of tech abuse.**

Children can be a gateway for perpetrators to control their partners, especially when former spouses are living apart. In the context of emerging technologies, smart, Internet-connected toys can become a means to track children as well as spouses behaviour [25]. The Online Harms White Paper refers to children's toys and baby monitors (Box 32, Page 83). However, there is no mention of how this technology can be misused in the context of domestic violence and abuse.

2. **Improve level of preparedness and awareness on tech abuse amongst victims/survivors as well as statutory and voluntary services.**

The Online Harms White Paper proposes that "all users, children and adults, should be empowered to understand and manage risks so that they can stay safe online" (Page 85). Such calls create expectations which can negatively affect vulnerable groups such as victims/survivors. Besides, the framing appears to make implicit assumptions about a person's personal autonomy, power, knowledge, and access.

As our research on technology-facilitated domestic abuse indicates that victims/survivors often feel to lack capacity staying safe online [1]. It echoes claims around insufficient awareness and tech-savviness amongst practitioners helping victims/survivors on the frontline. This includes statutory and voluntary services, such as police forces or refuges [2].

Thus, while we welcome the new Online Media Literacy Strategy, we believe it alone may not be enough to address the risk of technology-facilitated domestic and sexual violence and abuse. More needs to be done – including through increased funding for the sector – to help victims/survivors manage their own and their children's online safety and to advance statutory and voluntary services' tech abuse readiness.

3. **Shift responsibility to businesses to reduce the burden on victims/survivors and support services.**

One of the current measures put forward for the fulfilment of the duty of care is to "[d]irect users who have suffered harm to support" (p. 64). We welcome this measure and agree that "[c]ompanies should invest in the development of safety technologies to reduce the burden on users to stay safe online" (Summary, Page 12). However, we would like to see more

clarity on this process of giving access to support (such as our earlier indicated helpline) and receive a better understanding of the types of measures businesses will be expected to implement.

Conclusion

We encourage the UK Government to work on this Strategy with victims/survivors of domestic and sexual violence and abuse, and with the voluntary and statutory support services that work with victims/survivors. This way, the Online Harms White Paper as well as the Online Media Strategy can accurately represent the risks for victims/survivors of technology-facilitated abuse.

About the Gender and IoT Research Project

Gender and IoT is an interdisciplinary research project at UCL. The project team includes **Dr Leonie Maria Tanczer, Dr Simon Parkin, Dr Trupti Patel, Isabel Lopez-Neira, and Julia Slupska**. Gender and IoT is run in collaboration with the London Violence Against Women and Girls (VAWG) Consortium, Privacy International, and the PETRAS Internet of Things Research Hub. More information about the Gender and IoT research project, including relevant reports and previous consultation responses are available online: https://www.ucl.ac.uk/steapp/research/centres-and-institutes/digital-policy-laboratory/gender-and-iot

For any further information, please contact Dr Leonie Tanczer, l.Tanczer@ucl.ac.uk

[1] L. M. Tanczer, T. Patel, S. Parkin, and G. Danezis, “Response to the UK Government consultation ‘Transforming the response to Domestic Abuse’: The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT),” University College London, London, May 2018.

[2] L. M. Tanczer, I. Lopez-Neira, S. Parkin, T. Patel, and G. Danezis, “Gender and IoT (G-IoT) Research Report: The rise of the Internet of Things and implications for technology-facilitated abuse,” University College London, London, Nov. 2018.

[3] Communications Alliance Ltd, “G660:2018 Assisting Customers Experiencing Domestic and Family Violence Industry Guideline,” Communications Alliance Ltd, Sydney, Oct. 2018.

[4] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, “‘A Stalker’s Paradise’: How Intimate Partner Abusers Exploit Technology,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2018, pp. 667:1–667:13.

[5] M. Dragiewicz *et al.*, “Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms,” *Fem. Media Stud.*, vol. 18, no. 4, pp. 609–625, Jul. 2018.

[6] B. A. Harris and D. Woodlock, “Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies,” *Br. J. Criminol.*, Nov. 2018.

[7] A. Powell and N. Henry, “Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives,” *Polic. Soc.*, vol. 0, no. 0, pp. 1–17, Mar. 2016.

[8] N. Henry and A. Powell, “Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research,” *Trauma Violence Abuse*, p. 1524838016650189, Jun. 2016.

[9] I. Lopez-Neira, T. Patel, S. Parkin, G. Danezis, and L. M. Tanczer, “‘Internet of Things’: How abuse is getting smarter,” *Safe – Domest. Abuse Q.*, no. 63, pp. 22–26, Mar. 2019.

[10] J. Slupska, “Safe at Home: Towards a Feminist Critique of Cybersecurity,” *St Anthonys St Antonys Int. Rev.*, no. Whose Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace, 2019.

[11] R. Leitão, “Digital Technologies and Their Role in Intimate Partner Violence,” in *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2018, p. SRC11:1–SRC11:6.

[12] Y. Strengers, J. Kennedy, P. Arcari, L. Nicholls, and M. Gregg, “Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters,” in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA, 2019, pp. 645:1–645:13.

[13] B. O. eSafety Women, “Take the tour,” *Office of the eSafety Commissioner*, Jun-2019. [Online]. Available: http://www.esafety.gov.au/en/women/take-the-tour. [Accessed: 23-Jun-2019].

[14] Refuge and Safety Net, “Home Automation: Survivor Privacy Risks & Strategies,” *Refuge*, Mar-2019. .
[15] NNEDV, “Resources,” *National Network to End Domestic Violence*, Jun-2019. .
[16] N. Bowles, “Thermostats, Locks and Lights: Digital Tools of Domestic Abuse,” *The New York Times*, New York, 07-Aug-2018.
[17] E. Burden, “Husband used smart-home device to spy on wife,” *The Times*, 11-May-2018.
[18] P. Braithwaite, “Smart home tech is being turned into a tool for domestic abuse,” *Wired UK*, 22-Jul-2018.
[19] GSMA, “The Mobile Economy 2018,” GSM Association, unknown, 2019.
[20] R. Chatterjee *et al.*, “The Spyware Used in Intimate Partner Violence,” in *2018 IEEE Symposium on Security and Privacy (SP)*, 2018, pp. 993–1010.
[21] CIRCL, “Mission Statement,” *CIRCL*, unknown. [Online]. Available: https://www.circl.lu/mission/. [Accessed: 27-Jun-2019].
[22] Varni Na Internetu, “Področja zlorab,” *Varni na internetu*, unknown. .
[23] Department for Digital, Culture, Media and Sport, “Code of Practice for Consumer IoT Security,” Department for Digital, Culture, Media & Sport, London, Oct. 2018.
[24] P. Szewczyk, “Usability and Security Support Offered Through ADSL Router User Manuals,” *11th Aust. Inf. Secur. Manag. Conf.*, vol. Edith Cowan University, p. 2013, 2013.
[25] C. Bye and A. Khan, “Domestic violence technology summit hears prevalence of tech in violence,” *The Daily Telegraph*, London, 29-Nov-2016.
[26] M. Williams, J. R. C. Nurse, and S. Creese, “Privacy is the Boring Bit: User Perceptions and Behaviour in the Internet-of-Things,” in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 181–18109.
[27] S. Barth and M. de Jong, “The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review,” *Telemat. Inform.*, vol. 34, no. 7, pp. 1038–1058, 2017.
[28] A. R. Beresford, D. Kübler, and S. Preibusch, “Unwillingness to pay for privacy: A field experiment,” *Econ. Lett.*, vol. 117, no. 1, pp. 25–27, Oct. 2012.
[29] J. P. Carrascal, C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira, “Your Browsing Behavior for a Big Mac: Economics of Personal Information Online,” in *Proceedings of the 22Nd International Conference on World Wide Web*, New York, NY, USA, 2013, pp. 189–200.