TECH ABUSE

Gender and IoT Research Report

The rise of the Internet of Things and implications for technology-facilitated abuse

Leonie Tanczer
Isabel Lopez Neira
Simon Parkin
Trupti Patel
George Danezis

London, November 2018

PETRAS

London VAWG Consortium

PRIVACY INTERNATIONAL

Summary

Technology poses a risk to victims and survivors of sexual and domestic violence and abuse. This includes emerging technologies such as “smart”, Internet-connected devices, also known as the Internet of Things (IoT). Throughout our research, we have found that, at present, there is a lack of awareness and technical capacity to respond to technology-facilitated abuse both in statutory and voluntary support services. Therefore, we call for measures to increase the level of knowledge and competence of support services to respond to tech abuse, a “future-proofed” domestic violence and Internet security legislation, and for technology-facilitated abuse to be incorporated into support services risk assessments and safety plans. We also highlight the importance for both statuary and voluntary support services to collect data on the extent and nature of technology-facilitated abuse cases and to actively monitor changes in this evolving landscape.

The rise of tech abuse

Technology-facilitated abuse, so-called “tech abuse”, encompasses the ways in which technologies can be exploited to harass or control individuals [1] [2]. These include unwanted (sexual) attention, speech acts that cause fear and intimidation, image-based violations, and physical offenses [3]. The rapid change of technology gives perpetrators multiple tools to control people, which is of particular importance when looking at the power dynamics played out in intimate partner violence situations [4] [5]. The latter continues to affect primarily women and girls, with 1.2 million females in England and Wales having reported domestic abuse cases ending March 2017 [6].

Despite the rising uptake of technological devices on our day-to-day lives, there is still little exploration and response to the growing threats of tech abuse [3]. In recent years, distinct forms of online harassment and sexual abuse emerged [7] [8] [9], ranging from cyberstalking to online behavioural control or the use of spyware [10]. The UK domestic violence charity, Refuge, has warned about the rise of technology-facilitated abuse [11]. With more than 920 cases since January 2018 [12], women-centred organisations have begun to provide guidance and training on the safe use of digital technologies. Still, both statutory and voluntary support services recognise the demand for more support and resources to respond to tech abuse [13] [14]. At the same time, there have been calls aimed at technology vendors to prioritise the security and privacy needs of survivors and other vulnerable groups [15] [16] [17].

The impact of the Internet of Things

While many of the previous tech abuse efforts are concerned with “conventional” cyber risks such as abuses on social media platforms and restrictions to devices such as laptops and phones, the risk landscape is steadily transforming. In particular, the emergence of “Internet of Things” (IoT) technologies such as “smart’”, Internet-connected meters, locks, and cameras are of relevance and have so far been barely explored.

IoT is an umbrella term that reflects an evolution of different technologies across a whole spectrum of applications. These range from tiny sensors that collect humidity or temperature levels, to “gadgets” and household appliances such as “smart” fridges or thermostats, to complex systems such as connected and autonomous vehicles. What makes IoT devices unique is their connectivity. It allows different systems to be interlinked, creating an interdependent network with different devices basically “speaking” to each other [18] [19].

While many IoT systems at the moment require human action – such as through the pressing of a button or the activation through an app – they are expected to soon act without direct human intervention, by learning preferences and patterns through information gathered over time. Due to their range of functionalities, including their ability to be remotely controlled or to record videos and share location data, IoT devices have the potential to fundamentally change societal and business processes within and across sectors.

However, these technologies are also understood to create profound security, safety, and privacy risks and may be – due to their extensive functionalities – deliberately misused to spy on people, track their movements, or to exert control over them. In addition, IoT systems currently lack well-established security and privacy settings and are inherently designed based on the assumptions that all of their users trust each other. As such, they represent a new risk vector, especially for individuals who have already been subjected to tech abuse [19].

More of these devices are expected to be part of public and private spaces. According to estimates [20], the number of connected IoT devices worldwide will jump 12% on average annually, from nearly 27 billion in 2017 to 125 billion in 2030. Still, little research exists regarding the risks that may emerge from the rapid adoption of this technology in terms of domestic as well as sexual abuse.

About our research

"Gender and IoT" (G-IoT) is an interdisciplinary project at University College London (UCL). It analyses the evolving privacy and security risks of IoT systems in the context of domestic violence and abuse. The G-IoT team aims to provide guidance for services that engage with and help victims and survivors, such as women's charities, refuges, perpetrator programmes and police forces, as well as for IoT developers to consider the potential misuse of their devices and services. In order to develop these strategies, our research aims to understand:

1. The **role and impact** of IoT technologies on victims of domestic violence and abuse;
2. The **potential risk trajectories** that may arise from IoT devices and services;
3. And the **awareness and strategies** showed by victims and support services regarding the risks of IoT-related domestic violence and abuse.

In the next section, we present the main findings that we have identified as a result of our activities.

Findings

Throughout the course of our research, we uncovered a lack of awareness and capacity from support services to respond to tech abuse, and particularly to the risks posed by emerging technologies like IoT.

(1) Support services face shortcomings in existing tech abuse provisions

Statutory and voluntary support services are not yet equipped to respond to "conventional" forms of tech abuse, for example when it comes to advising survivors on how they can protect themselves against spyware or online harassment. This is concerning because an even stronger technical capacity will be needed to respond to IoT-facilitated tech abuse.

(2) There is a lack of awareness and technical capacity in support services to deal with IoT-facilitated tech abuse

We have uncovered a lack of awareness of the intersection between IoT and domestic abuse amongst both statutory and voluntary organisations. As we expect the uptake of IoT devices to become more widespread in the near future, the sector's alertness to these systems abilities and functionalities has to be raised.

(3) Tech abuse must be considered in policies and legislation

The risks of IoT associated with domestic violence and abuse are currently not considered in domestic abuse legislation as well as Internet safety and IoT security policies. Thus, the emphasis on mainstream technologies and platforms has to be expanded to foresee challenges and respond to the amplification of Internet-connected devices.

(4) Tech abuse is not considered in risk assessments and safety plans

We identified that tech abuse is currently not explicitly addressed in the risk assessment and frequently also the safety planning of victims and survivors. Besides, even when tech abuse is considered, the scope of this focus does not always account for emerging technologies such as the IoT.

(5) There is currently a lack of data on tech abuse

There is currently no UK-wide collection and assessment of tech abuse incidents. This makes it difficult to estimate the full scale and extent of the problem.

Recommendations

Based on our findings, we propose the following recommendations aimed at statutory and voluntary support services, tech vendors, and policy officials:

(1) Domestic violence and cybersecurity practitioners must work in tandem

Support services must closely collaborate with cybersecurity practitioners for an efficient response to tech abuse. This can be done through the establishment of dedicated tech abuse units, and/or through a hotline that could sit within the National Cyber Security Centre (NCSC). The tech sector must also have a role in foreseeing and actively preventing the misuse of their systems by mitigating these risks through enhanced privacy and security measures.

(2) Support services must have the capacity to deal with the threat of IoT-facilitated tech abuse

In addition to facing shortcomings in their overall response to tech abuse, support services should be prepared for the rising uptake of IoT devices. This could be done through development of training, guidance, and resources to upskill the sector.

(3) Domestic abuse and Internet security legislation must be "future-proofed"

Given the expected growth of Internet-connected devices, legislation such as the upcoming Internet Safety Strategy and the Domestic Abuse Bill, must be future-proofed to deal with risks of domestic abuse associated with IoT technologies.

(4) The risk of tech abuse must be incorporated into risk assessments and safety planning processes

Risk assessments and safety plans should include tech and IoT abuse to sufficiently identify and respond to this threat. This could also help to monitor the extent and changing nature of tech abuse.

(5) More data must be collected to estimate the scale of the problem, and to monitor changes over time

Police forces and frontline staff are encouraged to amend their reporting patterns to collate information about the number and types of technologies that are being used in abuse cases. This would allow for a systematic monitoring of tech abuse and could point towards shortcomings across different technologies and platforms.

About us

G-IoT is an **interdisciplinary research project** at UCL. The research team includes Dr Leonie Tanczer, Dr Simon Parkin, Dr Trupti Patel, Isabel Lopez Neira, and Professor George Danezis. The project was funded by a Social Science Plus award from UCL's Collaborative Social Science Domain, the NEXTLEAP project, and a UCL Public Policy grant.

G-IoT runs in collaboration with the London VAWG Consortium, Privacy International, and the PETRAS IoT Hub.

Our work was, amongst others, featured in the BBC, WIRED UK, the Evening Standard, and The Verge.

If you want to stay in touch and keep informed about our research progress as well as ongoing developments in this emerging research field, you can follow our monthly newsletter accessible through our website.

Further information

You can find more information about tech abuse as well as IoT-facilitated abuse in our guide and resource list.

References

[1] D. Freed, J. Palmer, D. Minchala, K. Levy and T. Ristenpart, ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology," *CHI,* 2018.

[2] D. Woodlock, "The Abuse of Technology in Domestic Violence and Stalking," *Violence Against Women,* vol. 23, no. 5, pp. 584-602, 2017.

[3] N. Henry and A. Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," *Trauma, Violence & Abuse,* pp. 1-14, 2016.

[4] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart and N. Dell, "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," Vols. 1, Article 46, 2017.

[5] M. Dragiewicz, J. Burgess, A. Matamoros-Fernandez, M. Salter, N. P. Suzor, D. Woodlock and B. Harris, "Technology facilitated coercive control: Domestic Violence and the competing roles of digital media platforms," *Feminist Media Studies,* vol. 18, no. 4, pp. 609-625, 2018.

[6] Office for National Statistics, "Domestic abuse in England and Wales: year ending March 2017.," Office for National Statistics, 2017.

[7] Law Commission, "Abusive and Offensive Online Communications.," London, 2018.

[8] N. Suzor, M. Dragiewicz, B. Harris, R. Gillet, J. Burgess and T. Van Geelen, "Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online," *Policy & Internet,* vol. 9999, no. 9999, pp. 1-20, 2018.

[9] J. K. Peterson and J. Densley, "Cyber violence: What do we know and where do we go from here?," *Aggression and Violent Behaviour,* vol. 34, pp. 193-200, 2017.

[10] R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy and T. Ristenpart, "The Spyware Used in Intimate Partner Violence," *IEEE Symposium on Security and Privacy,* pp. 441-458, 2018.

[11] Refuge, “Tech Abuse,” [Online]. Available: https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse/. [Accessed 5 November 2018].

[12] M. Blunden, “Abusive partners use home technology to stalk and abuse women,” 28 August 2018. [Online]. Available: https://www.standard.co.uk/tech/abusive-partners-use-home-technology-to-stalk-and-abuse-women-study-shows-a3921386.html.

[13] Snook, Chayn and SafeLives, “Tech vs Abuse: Research Findings,” 2017.

[14] A. Powell and N. Henry, “Policing technology-facilitated sexual violence against adult victims: police and service sector perspective,” *Policing and Society,* vol. 28, no. 3, pp. 291-307, 2018.

[15] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill and S. Consolvo, “Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse,” *CHI,* 2017.

[16] T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill and S. Consolvo, “Security and Privacy Experiences and Practice of Survivors of Intimate Partner Abuse,” *IEEE SEcurity & Privacy,* vol. 15, no. 5, pp. 76-81, 2017.

[17] B. Arief, P. L. Kovilla, M. Emms and A. van Moorsel, “Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse,” *Proceedings of the 13th Workshop on Privacy in the Electronic Society,* pp. 201-204, 2014.

[18] L. Tanczer, I. Brass, M. Elsden, M. Carr and J. Blackstock, “The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape,” in *Rewired: Cybersecurity Governance*, Hoboken, Wiley, forthcoming.

[19] P. Taylor, “Internet of Things: realising the potential of a trusted smart world,” Royal Academy of Engineering, London, 2018.

[20] IHS Markit, “The Internet of Things: A movement, not a market,” Englewood, United States, 2017.