This is an accepted article published in
Safe – The Domestic Abuse Quarterly

Please cite as:

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter. Safe – The Domestic Abuse Quarterly, (63), 22-26.

https://www.womensaid.org.uk/research-and-publications/safe/

‘Internet of Things’: how abuse is getting smarter

From home thermostats you can control from your car, to home assistants ready to organise your diary at a spoken word, technology is playing a more central role in our daily lives. However, while networked home devices provide many advantages, they also offer abusers an abundance of opportunities to control, harass and stalk their victims. The Gender and Internet of Things project at University College London has been investigating how these devices are being misused, and what support survivors and services need to navigate these emerging risks.

By Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer, from the Gender and IoT project at University College London

Over recent years, technology has been shown to pose a new risk factor to victims and survivors of sexual and domestic violence and abuse. With the use of smartphones and the internet becoming more widespread, technology-facilitated abuse, so-called ‘tech abuse’, has become a prevalent issue. This dynamic of abuse, however, is changing and further expanding. With the proliferation of a diverse range of ‘smart’, internet-connected devices — also known as the Internet of Things (IoT) — the number of systems which may be used for abuse is rising. Examples of such IoT devices include smart speakers such as the Amazon Echo which can be controlled through voice activation, smart locks that can be opened with an app, or smart heating systems which allow for remote control.

Researchers from the Gender and IoT (G-IoT) project at University College London (UCL) are investigating how these new IoT devices may be used against victims and survivors of domestic violence and abuse. In May 2018, Ross Cairns was convicted of stalking his estranged wife Catherine, after he hacked into the smart home hub installed in the kitchen to spy on her. Using a mobile app, he logged into the audio facility on the iPad system display and listened to her conversations with her mother. The case was one of the first recorded instances of IoT technology — in this instance, a wireless system used to control the lighting, central heating and alarm — being used to abuse a partner.

The team is also studying the capacity of statutory and voluntary support services to cope with the expected increase in cases reported as a result of IoT-facilitated abuse. This work is being conducted alongside the London Violence Against Women and Girls Consortium, consisting of 29 support organisations across London, the PETRAS IoT Hub, a consortium of nine UK universities

studying IoT technologies, and Privacy International, a digital rights group working at the intersection of modern technologies and rights.

In this article, the G-IoT team calls attention to the evolving role of emerging technologies in cases of domestic and sexual violence and abuse and presents research findings that highlight the need for action from legislators, technologists, and support services.

"... it's only since I've got your email that we're starting to have discussions about 'How prevalent is this for our client group? What are we doing for them?' "

A frontline worker

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, image-based violence, emotional manipulation, or coercive offences[3]. The rapid growth and adoption of new technologies gives perpetrators multiple tools to control and manipulate people, which is of particular importance when looking at the power dynamics played out in situations of intimate partner violence[4,5].

Despite the rising uptake of manifold technologies in our day-to-day lives, there is still little exploration and research on the growing threats these systems may bring to some of the most vulnerable groups within society. In 2017, Women's Aid published the All-Party Parliamentary Group on Domestic Violence and Abuse report[6] on online abuse, calling for the government, judiciary and relevant agencies to recognise the harm caused by it. In recent years, distinct forms of online harassment and sexual abuse have emerged[7,8,9], ranging from cyberstalking to surveillance through the usage of spyware (i.e., software that aims to gather information about a person without their knowledge)[10]. The charity Refuge has documented more than 920 tech abuse cases since January 2018[11,12], with many support organisations having slowly 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 this increasing problem[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].

The impact of the Internet of Things

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' thermostats or toys, to complex systems such as connected and autonomous vehicles. What makes IoT devices unique is their connectivity. It allows different devices to be linked, creating a network of different devices basically 'communicating' with each other[17,18]. IoT, thus, goes beyond smartphones, laptops, and tablets. It means an expansion of internet-capabilities into devices that either did not exist before (i.e. smart speakers such as Amazon Echo), or were previously 'offline' tools (i.e. smart kettles, smart fridges).

While many IoT systems at the moment require human action – such as through the pressing of a button or activation through an app – they are expected to eventually 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 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, with the capacity – due to their extensive functionalities – to deliberately be misused to spy on people, track their movements, exert control over them or coerce them. In addition, IoT systems currently lack well-established security and privacy settings and are inherently designed based on the assumptions that all of the users in a home trust each other. In instances in which intimate partner violence is being enacted, this assumption of trust poses a problem, as IoT systems can be used to facilitate abuse[18].

To date, most tech abuse research efforts have been concerned with 'conventional' cyber risks such as harassment and abuse on social media platforms, and restrictions to devices such as laptops and phones. However, the sources of tech abuse are steadily increasing. In particular, the emergence of internet-connected locks, cameras, and toys will offer coercion and manipulation opportunities against victims and survivors. The term 'gaslighting' originated from Patrick Hamilton's 1938 play *Gas Light,* where a woman is manipulated by her husband to doubt her perception of the environment around her and question her own sanity. Now this behaviour can happen through the touch of a mobile phone screen, whether it is to adjust the temperature of a room from miles away, or to boil a kettle to remind someone you are watching.

More of these devices are predicted to be part of public and private spaces[19]. According to estimates, the number of connected IoT devices worldwide will jump 12% on average annually, from nearly 27 billion in 2017 to 125 billion in 2030[19]. Still, little research exists regarding the risks that may emerge from the rapid adoption of these interdependent technologies in terms of domestic, as well as sexual, abuse.

The G-IoT team consequently proposes a range of recommendations that draw on focus groups and interview data conducted throughout the research.

The importance of collaboration: knowledge exchange with support services

In the course of the study, the team has identified that support services tend to feel a lack of preparedness or even awareness of the risks of devices and emerging technologies such as IoT. From the start of the project, the team has therefore engaged very closely with the sector, both through training and events, and has upheld an active commitment to co-develop the research with all stakeholders in order to explore charities' interests and needs.

Over the past year, two workshops have been held to begin discussions with frontline workers about their experiences of tech abuse and to raise awareness of issues they may have to face in the near future.

In November 2018, the Gender and IoT team held a 'CryptoParty', where support services were offered digital security training focussed on the themes of 'How to secure your data securely', 'Browser security', 'Secure communication', 'Detecting compromised accounts', and 'Staying safe when using your phone'. Attendees took part in one of the sessions which offered hands-on advice and training. This was followed by a panel discussion comprising academic, industry, support service, and policy representatives. This event aimed to lower the barrier for the charitable sector to prepare for the challenges they may have to face in the near future concerning new forms of tech abuse.

"[We need] more comprehensive understanding of potential issues from IoT issues. More effective support to my member organisations regarding same. Simple accessible materials setting out issues in non 'tech' language."

A support worker

The team is dedicated to supporting charities and frontline workers and have produced diverse resources, including a resources list and a guide as well as an information leaflet for policy makers. The G-IoT team also responded to the UK government domestic abuse consultation and emphasised the need to prepare the sector for these upcoming technological transformations. All of these documents are available on the project webpage. They hope to shape a more timely response to individuals in need, and to work collectively towards reducing the risks of tech abuse in our society.

The response received thus far has been extremely positive and the team is keen to engage further with the community, which has shown an eagerness to understand the issues and upskill on tech-facilitated abuse. All of the events have shown the possibilities of bringing together the tech community and support services, and enabling them to have the discussions needed to help address an emerging phenomena.

Findings

Through focus group discussions and interviews, the G-IoT team has made the following key findings:

Support services face shortcomings in their ability to respond or advise on tech abuse.

Support services have limited capacity and resources to increase their awareness and technical capacity to deal with IoT-facilitated tech abuse.

Tech abuse is not explicitly considered in all risk assessments and safety plans.

There is currently a lack of data on tech abuse.

Recommendations

Based on the findings, the team has proposed the following recommendations aimed at statutory and voluntary support services, tech vendors, and policy officials:

Domestic violence and cybersecurity practitioners must work in tandem. The CryptoParty held by the project team was brought about through this concern.

Services must be supported to have the capacity to deal with the threat of IoT- facilitated tech abuse.

Domestic abuse and internet security legislation must be 'future-proofed'.

Tech abuse must be considered in policies and legislation.

The risk of tech abuse must be incorporated into risk assessments and safety planning processes.

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

Contact the G-IoT team!

If you would like to learn more about the G-IoT research project or participate in a confidential one-to-one research interview, please visit their webpage where you find the research team's contact details, helpful guides and resources, as well as a link to subscribe to their monthly newsletter.

Notes

1 D. Freed, J. Palmer, D. Minchala, K. Levy and T. Ristenpart (2018) '"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology', *CHI Conference on Human Factors in Computing Systems*. ACM.

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

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

4 D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart and N. Dell, (2017) 'Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders,' *Proceedings of the ACM on Human-Computer Interaction* Vols. 1, Article 46.

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

6 Women's Aid (2017) *Tackling domestic abuse in a digital age: A Recommendations Report on Online Abuse by the All-Party Parliamentary Group on Domestic Violence.* Women's Aid.

7 Law Commission (2018) *Abusive and Offensive Online Communications* London.

8 N. Suzor, M. Dragiewicz, B. Harris, R. Gillet, J. Burgess and T. Van Geelen (2018) 'Human Rights by Design: The Responsibilities of Social Media Platforms to Address Gender-Based Violence Online,' *Policy & Internet*.

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

10 R. Chatterjee, P. Doerfler, H. Orgad, S. Havron, J. Palmer, D. Freed, K. Levy, N. Dell, D. McCoy and T. Ristenpart (2018) 'The Spyware Used in Intimate Partner Violence,' *IEEE Symposium on Security and Privacy,* pp. 441-458.

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

12 M. Blunden [Online 28 August 2018] *Abusive partners use home technology to stalk and abuse women*. 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, (2017) *Tech vs Abuse: Research Findings*.

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

15 T. Matthews, K. O'Leary, A. Turner, M. Sleeper, J. P. Woelfer, M. Shelton, C. Manthorne, E. F. Churchill and S. Consolvo (2017) 'Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse,' *CHI Conference on Human Factors in Computing Systems*. ACM.

16 B. Arief, P. L. Kovilla, M. Emms and A. van Moorsel (2014) '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.

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

18 P. Taylor (2018) *Internet of Things: realising the potential of a trusted smart world.* Royal Academy of Engineering, London.

19 IHS Markit (2017) *The Internet of Things: A movement, not a market*. Englewood, United States.