Good Practice Briefing

Technology and Violence Against Women – Helping or Harming?

April 2019

AVA (Against Violence and Abuse)

The Foundry, 17 Oval Way, London SE11 5RR

Tel: 020 37525535 Email: info@avaproject.org.uk

Website: www.avaproject.org.uk Twitter: @AVAproject

Registered charity no. 1134713. Registered company no. 7092249.

Contents

Contents

ASCENT - Support services to organisations

Ascent is a partnership within the London Violence Against Women and Girls (VAWG) Consortium, delivering a range of services for survivors of domestic and sexual violence, under six themes, funded by London Councils.

ASCENT – Support services to organisations, is delivered by a partnership led by the Women's Resource Centre (WRC) and comprised of five further organisations: AVA, IMKAAN, RESPECT, Rights of Women, and Women and Girls Network.

This second tier support project aims to address the long term sustainability needs of organisations providing services to those affected by sexual and domestic violence on a pan-London basis.

The project seeks to improve the quality of such services across London by providing a range of training and support, including:

- Accredited training
- Expert-led training
- Sustainability training
- Borough surgeries
- BME network
- One-to-one support
- Policy consultations
- Newsletter
- Good practice briefings
- Good practice briefings

The purpose of the good practice briefings is to provide organisations supporting those affected by domestic and sexual violence with information to help them become more sustainable and contribute with making their work more effective. For more information, please see: www.thelondonvawgconsortium.org.uk

This practice briefing was produced by AVA (Against Violence and Abuse) on behalf of the Ascent London VAWG Consortium. AVA is a leading UK charity aimed at ending gender based violence and abuse. We strive to improve services through our learning, resources and consultancy, and end violence against women and girls through our policy, research and prevention work. We have specific expertise on multiple disadvantage and children and young people.

For more information about AVA, please see: www.avaproject.org.uk

Introduction

In today's world, technology is unavoidable and constantly changing. Although many forms of technology offer services and survivors opportunities for support and safeguarding, they also offer perpetrators a new toolbox of ways to stalk, exploit, isolate and control women and children. This briefing paper aims to present an overview of the current and emerging risks, and considers potential opportunities and safety planning tips. As new forms of tech emerge daily, all service providers should aim to keep up to date with the latest risks and developments. The resources section at the end of the briefing provides a useful list of organisations and tools to help with this.

Prevalence of Online Abuse

A recent survey by Safelives and Comic Relief[1] found that 47% women who had experienced abuse had also had their online activity monitored by their partner and 25% said they did not know if this was happening or not (highlighting the covert nature of some of the ways victims can be monitored and controlled online). The SafetyNet project in the US found 97% reported that the survivors they are working with experienced harassment, monitoring, and threats by abusers through the misuse of technology.

Online harassment is intersectional, often incorporating sexism, racism, homophobia, and other forms of oppression. Abusers may use a vast array of online tactics to harass their victims[1].

Examples of How Technology Can Be Used to Abuse

There are a range of tactics that may be used by abusers online, the list below is not exhaustive, but covers some of the most common:

- Demanding passwords
- Constant checking of phone/social media
- GPS tracking apps
- Threats via messaging, email, social media
- Identify theft
- Using apps to gain access to a webcam
- Threats to share images/'Revenge porn'
- The use of 'spyware' to monitor someone online
- Setting up alias accounts
- Repeated messaging
- Hidden cameras
- Recording devices in children's toys
- The use of digital devices to record and gather information
- The use of wireless devices to control things such as lighting

[1] Comic Relief (2017) Tech Vs Abuse

The Internet of Things

The Internet of Things (IoT) is an umbrella term that describes interconnected 'things' and systems which are the direct extension of the internet into a range of physical objects and devices.[2] Basically, this includes products which have become digitally 'smart' such as Amazon Echo, Google Home, Philips Hue, Fitbits etc. Again, these devices offer perpetrators additional ways to monitor, control and abuse victims.

A team at UCL have been working with the London VAWG consortium to research IoT risks and have found evidence of these devices being capable of sharing and tracking locations, audio and video functionality and recording, viewing purchasing history and voice commands, remote controlling of heating and lighting etc. Given that the government estimates every household will have 15 internet connected devices by 2020, it is crucial that service providers understand how these tools may be used as part of a perpetrators abuse and how to advise victims on staying safe. The UCL team have developed some useful resources for practitioners (see resource list).

Cyber-Stalking

Cyber, or digital, stalking is the use of the internet, email or other electronic communication to stalk someone. This is an offence under the 2012 Protections of Freedom Act which amended the Protection from Harassment Act 1997. However, cyber-stalking is often classified as 'malicious communications' and does not take into account the course of conduct (conduct that occurs on two or more occasions) which would classify it as stalking.

In March 2019, The Stalking Protection Bill received Royal Assent and will see the introduction of new Stalking Protection Orders - a civil order that police can apply for with the flexibility to impose both restrictions and requirements on perpetrators which will carry a criminal penalty for those that breach them. The police will apply for the order, so the burden of going through the process does not lie with a vulnerable victim[3].

It is crucial that service providers and police are using the right language and calling this behaviour stalking or coercive control, in order to lead to the correct charge for the perpetrator and support for the victim.

The Suzy Lamplugh Trust found that 36.8% of people stalked, were stalked online, and of those people, 43% withdrew from online activity or social media. When online stalking was the only form of abuse, only 9.8% was reported to the police. The cyber-stalking led to victim's feeling afraid, moving home, not using their phone or answering the door. High levels of trauma including PTSD, anxiety and depression are also common.

[2] Tanczer, L. et al. The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R.Ellis & V. Mohan (Eds.), Cybersecurity Governance. Wiley.
[3] Home office (2019) Government backed Stalking Protection Bill receives Royal Assent https://www.gov.uk/government/news/government-backed-stalking-protection-bill-receives-royal-assent

SmartPhone Apps

Smartphone apps are becoming increasingly common as a way of addressing domestic and sexual violence and stalking in a variety of ways. They can be used to provide information and awareness, to identify risks and abuse or to store and/or share information with other people if someone is in danger. One study found[4] that 49% of apps designed to help victims of abuse were some form of panic alarm or danger alert system.

Many of these apps are popular with victims of abuse and are recommended by service providers. However, as with most forms of technology (even if the apps are disguised as a more generic app), there is also the possibility that they can be found and misused by perpetrators and put the victim at more risk. Another criticism is that these apps require women to do their own 'safety work'[5] and invest money, time and effort into 'keeping themselves' safe. Whilst there is certainly value in many of these apps, services and victims must be aware of any potential safety concerns.

There are guides in the resource section with tips for the safe development and use of apps.

Opportunities for Support

As well as providing many opportunities for perpetrators to control, abuse and stalk, when used safely, there are many ways technology can offer opportunities for support for victims and services. These include: blogs written by survivors which can inspire and empower others, online support groups and forums, online chats and 1:1 sessions (many charities offer this service now including rape crisis), awareness raising campaigns (such as the Home Office 'disrespect nobody' campaign on teenage relationship abuse) and the use of gaming to raise awareness about domestic abuse and stalking.

Funders such as Comic Relief and others have developed specific funding streams for organisations to develop digital products and services which play a supportive role in the context of domestic violence and abuse, whilst minimising the associated risks.

[4] Westmarland et al (2013) Protecting Women's Safety: The use of smartphone apps in relation to domestic and sexual violence. Durham University

[5] Kelly, L. (2013) Thinking in 10s: what we have learnt, what we need to know and do, inaugural lecture at the launch of the Durham Centre for Research into Violence and Abuse, Durham University, 16th May 2013.

Top Tips and Safety Planning Advice

There can be many evidential opportunities with digital abuse, as these activities will usually leave a digital footprint. However, it is important that the abuse can be attributed back to the perpetrator. Every police force will have a cyber-crime unit and a digital media investigator who can advise on the best way to retrieve, retain and store evidence. It is vital that services are equipped with up to date knowledge about current and emerging risks involving technology and make sure they are a routine part of any risk assessment and safety planning.

Below are some tips to bear in mind when advising victims and when developing safety plans:

- Review what information exists about the victim online (this can also be useful for practitioners to do for themselves)
- Ensure all devices have updated antispyware software installed and turned on
- Keep all privacy settings on social media accounts up to date
- Turn off all GPS and location sharing settings
- Regularly change e-mail and passwords
- Avoid sharing photos that may identify your location or any personal information
- Request to be notified before anyone can check you in or tag you on facebook
- Make sure wireless hubs and routers have security options turned on
- All risk assessments to routinely ask about experiences of digital abuse
- Collect and save any evidence from social media sites (prior to asking for it to be removed)
- Keep recordings of calls and voicemails
- Document and report incidents

Conclusion

This briefing paper has highlighted that there are many ways technology can be used to abuse, control and stalk. This is a growing area of concern and despite the welcome recent research, legislation and funding opportunities, this is an ever-changing field which services, commissioners and funders need to stay up to date with so they are better equipped to protect and support victims.

It is also important to remember, that technology can also offer opportunities for information, protection and support and these should be further funded and explored with appropriate consideration given to potential risks.

References

Comic Relief (2017) *Tech Vs Abuse*

Kelly, L. (2013) *Thinking in 10s: what we have learnt, what we need to know and do,* inaugural lecture at the launch of the Durham Centre for Research into Violence and Abuse, Durham University, 16th May 2013.

Home office (2019) *Government backed Stalking Protection Bill receives Royal Assent,* London. Available at https://www.gov.uk/government/news/government-backed-stalking-protection-bill-receives-royal-assent

Tanczer, L. et al.(2018) *The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape*. In R.Ellis & V. Mohan (Eds.), Cybersecurity Governance. Wiley.

Westmarladn et al (2013) *Protecting Women's Safety: The use of smartphone apps in relation to domestic and sexual violence.* Durham University. Available from; https://www.academia.edu/34176535/Protecting_Women_s_Safety_The_use_of_smartphone_apps_in_relation_to_domestic_and_sexual_violence

Appendix 1- Resources

Refuge – Tech Abuse (incudes safety tips and log sheets)
https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/

UCL – Internet of Things Research (includes research, guides and resource lists)
https://www.ucl.ac.uk/steapp/research/centres-and-institutes/digital-policy-laboratory/gender-and-iot

Tech vs Abuse - a collaborative research study about the use of digital tools to support people affected by domestic abuse. The project is supported by various institutions, including Comic Relief, Chayn, SafeLives, and Snook.
https://www.techvsabuse.info/

Take Back the Tech - a global campaign that connects the issue of violence against women* with emerging technologies. The website offers safety roadmaps and information on cyberstalking, hate speech and blackmail.
https://www.takebackthetech.net/

DIY Cybersecurity for Domestic Violence - A guide developed by Hack Blossom, an activists and artists' platform concerned with digital rights. The guide includes threat scenarios and provides strategies to keep safe online.
https://hackblossom.org/domestic-violence/

Choosing and Using Apps: Considerations for Survivors
https://www.refuge.org.uk/wp-content/uploads/2018/11/nnedv-refuge-app-considerations-survivors-2014.pdf

The National Stalking Helpline - run by Suzy Lamplugh Trust.
0808 802 0300

Getsafeonline - Provides advice on all aspects of computer and internet use including advice for using chat rooms, social networking, viruses, spam and safe shopping online. They have a page dedicated to cyberstalking
www.getsafeonline.org/protecting-yourself/cyberstalking

Facebook – how to report abuse on Facebook
https://www.facebook.com/help/contact/274459462613911

Tech Safety - exploring technology in the context of intimate partner violence, sexual assault, and violence against women. Includes a toolkit and app.
https://www.techsafety.org/

App Safety – Tips for the safe development and use of smartphone apps
https://www.techsafety.org/appsafetycenter

Chayn - co-designed resources with survivors of abuse from around the world.
https://chayn.co/