Digital Economy Bill

Women's Aid Evidence to the Public Bill Committee

25 October 2016

Introduction and summary

1. Women's Aid is the national charity working to end domestic abuse against women and children. We are a federation of over 220 organisations, who provide more than 300 local lifesaving services to women and children across the country. We have been at the forefront of shaping and coordinating responses to domestic violence and abuse through practice for over 40 years. Women's Aid campaigns for better support for women and children, provides training and resources for professionals, and delivers a package of vital 24 hour lifeline services through publications, websites and the National Domestic Violence Helpline in partnership with Refuge. We empower survivors by keeping their voices at the heart of our work, working with and for women and children by listening to them and responding to their needs.

2. Women's Aid warmly welcomes the opportunity to provide written evidence to the Public Bill Committee scrutinising the Digital Economy Bill. The Bill introduces a range of measures related to the digital economy – including age verification for online pornography and a new statutory code for direct marketing. We restrict our evidence to the area of digital safety and online abuse, and the experiences of survivors of domestic abuse in this regard.

3. In summary, our evidence sets out background information on the nature and impacts of online abuse, recommends that the Bill introduce a statutory code of practice for internet safety, and sets out considerations for how such a framework would protect survivors of domestic abuse online.

Background

4. The Government states that the law in this area is clear – what is illegal offline, is illegal online. However, the reality for survivors of domestic abuse when using online and digital platforms, services and products does not currently reflect this statement.

5. Many women experiencing domestic abuse are not only abused offline but are abused, harassed, and stalked online by their partners or ex-partners. Online abuse is the use of the internet or any other electronic means to direct abusive, unwanted and offensive behaviour at an individual or group. The internet and other electronic means are also used to stalk and harass – behaviour which is persistent, unwanted and causes fear to a victim. As the recently published Crown Prosecution Service (CPS) Guidelines on prosecuting cases involving communications sent via social media make clear,[1] online and digital abuse, stalking and harassment takes many forms – including behaviours such as:

- Monitoring of social media (such as Facebook or Twitter), messages or emails.
- Sending abusive, menacing or upsetting messages or threats on social networks, email and chatrooms – 'trolling'.
- Spreading lies or personal information about the person online.
- Creating a website or online groups to harass or abuse.
- Creating fake accounts, hijacking and stealing online identities.

[1] Crown Prosecution Service, Guidelines on prosecuting cases involving communications sent via social media, October 2016.

- Sharing private photos or videos online without consent – "revenge pornography" and image base sexual abuse.
- Posting "photoshopped" images of persons on social media platforms.
- "Baiting", or humiliating peers online, by labelling them as sexually promiscuous.
- Hacking into social media accounts, and then monitoring and controlling the accounts.
- Spamming (where offenders send victims multiple junk emails) and sending electronic viruses.
- Using technology for surveillance – including :
  - The use of GPS, other geolocator software, or spyware to track movements;
  - The use of applications ('apps') such as 'Find your Friends', or apps intended for tracking exercise, which can be used by perpetrators to monitor survivors.

6. Online abuse is a very real and present threat for women survivors of domestic abuse. It typically forms part of a pattern of coercive and controlling behaviour, and encompasses various forms of abuse – including physical, financial and sexual. Perpetrators of domestic violence now routinely use technology and social media to commit crimes, exerting the desire to control and instilling fear into those they victimise. The internet can be used as a vehicle for coercive control, enabling perpetrators to gather more information and data on their victims and increases opportunities to abuse, humiliate, threaten and control. Recent convictions under the new offence of coercive and controlling behaviour, as reported on by the CPS, show that perpetrators are monitoring victims through online and digital tools, and controlling victims through social media and online activity.[2]

7. In a 2013 Women's Aid survey of survivors of domestic abuse, 45% reported that they had experienced abuse online during their relationship.[3] A 2015 survey conducted by Women's Aid England with 693 survivors of domestic violence, who had been abused online by their partners or ex-partners, further found that:
   - For 85% of respondents the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline.
   - Nearly a third of respondents (29%) experienced the use of spyware or GPS locators on their phone or computers by a partner or ex-partner.
   - For half (50%) of respondents the online abuse they experienced also involved direct threats to them or someone they knew – and nearly a third of those respondents who had received threats stated that, where threats had been made online by a partner or ex-partner, they were carried out.

8. Survivors of domestic abuse are not routinely able to access the same protection from an abuser online, as they can offline. Criminal or civil sanctions, such as a Domestic Violence Protection Orders, Domestic Violence Protection Notices or Non-Molestation Orders, which restrain a perpetrator from contacting the victim, do not automatically prohibit online or digital contact – such as through emails, messages or social media. While revisions to the legislation on Ancillary orders are out of scope of this Bill, it is important to note that the protections and safety measures currently accorded to victims of domestic abuse online and offline differ significantly.

9. Women's Aid considers that improvements to the Digital Economy Bill would help to tackle this issue, and support parity of protection between online and offline forms of domestic abuse.

---

[2] Crown Prosecution Service, Violence Against Women & Girls Newsletter, Issue no 18, June 2016

[3] Women's Aid, Virtu*al World, Real Fear: Women's Aid Report into online abuse, harassment and stalking* (Bristol: 2014) https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

Current protections against online abuse

10. In considering how to improve the current prevention and response to online abuse, and protect victims of domestic abuse from it, Women's Aid echoes the statement of the Rt Hon Mrs Maria Miller MP in the second reading debate on the Bill:

    "There is an opportunity for better support to be provided to victims of online abuse…We must be clear that we will not tolerate the sort of abuse that has become routine in the past. We need to ensure that there is a co-ordinated approach to the reporting of online abuse, that we design out such abuse from products from the get go and that there is quick action to remove and sanction those who commit online abuse."[4]

11. Under current European Union legislation, digital intermediary service providers – such as social media platforms – are "*not liable for the content they hold and transmit passively*". Online abuse is currently tackled is through voluntary and self-regulatory action, resulting in a varied range of approaches across the industry. Women's Aid notes that best practice examples for preventing and tackling online abuse are already established – companies such as Facebook, Twitter, Instagram and Google have established quick and effective reporting procedures that help to protect victims and remove the onus on survivors to remove themselves from social media platforms. Many providers adhere to voluntary standards for best practice, such as the ICT Coalition for Children Online's Six Principles, and belong to partnerships that develop best practice – such as the UK Council for Child Internet Safety (UKCCIS).

12. However, there is currently no clear framework for the prevention and response to online abuse across the industry as a whole. There remains considerable variation in how effectively providers prohibit, enable reporting of, and respond to, online abuse – for example:
    - There is currently no consistency on how online providers define and prohibit online abuse within their terms and conditions and associated user guidance, and how this relates to the law on domestic abuse.
    - There are no common or minimum standards for online platforms for in-built reporting functions, which are required in order to: enable victims to directly report from the abusive content; specify the abuse as an incident of domestic abuse; and support victims by restricting their exposure to online abuse after they have reported it.
    - There are no common procedures for online providers for the effective prevention and response to the crime – such as:
        - a prohibition on the use of multiple accounts in the case of online abuse;
        - guidelines for location services – which are a significant concern, as apps increasingly require users to identify their location, and can enable perpetrators to track and monitor survivors more easily;
        - guidelines for how default settings can be used to improve safety;
        - requirements for training and expertise within support teams, to identify and handle cases of domestic abuse;
        - Established procedures for how providers handle, store and share evidence of online abuse, which is vital for the prosecution and conviction of perpetrators.

[4] Second Reading of the Digital Economy Bill, 13th September 2016, https://hansard.parliament.uk/commons/2016-09-13/debates/16091326000001/DigitalEconomyBill

A Code of Practice for Internet Safety

13. Clause 77 of the Bill establishes a code of practice for direct marketing to strengthen enforcement action. The statutory code aims to improve standards among direct marketers, by placing an obligation on organisations to adhere to the Direct Marketing Guidance of the Information Communications Office (ICO) and strengthening the ICO's powers to take enforcement action against a breach. Women's Aid believe that a code of practice for improving internet safety and tackling online abuse is as important as a code of practice for direct marketing, which aims to tackle nuisance calls and texts.

14. Women's Aid recommend that the Bill introduce a statutory code of practice for the purposes of internet safety. This would build on similar proposals suggested by organisations such as the NSPCC – who have proposed a code of practice to protect the safety and wellbeing of children online, that would apply consistently to social networks, intermediary service providers, mobile telecommunication companies and other communication providers.[5]

15. To ensure effective online protection for survivors of domestic abuse, Women's Aid recommend that a statutory code of practice for internet safety:
    - **Is developed in partnership with a range of stakeholders,** including survivors of online and domestic abuse, support services, organisations such as Women's Aid, academic experts, and the industry.
    - **Establishes common standards for the prohibition of online abuse,** which are aligned with the revision of the CPS guidelines on online abuse and the Law Commission's current consideration of the law on online communications.[6]
    - **Establishes minimum standards for the prevention and identification of, and response to, online abuse,** with specific reference to the standards of service that survivors of domestic abuse can expect. The standards would cover areas including: in-built reporting mechanisms; multiple accounts; guidelines for location services and default security settings; training and expertise for support staff; and how evidence is handled, stored and shared.
    - **Supports the prevention of online abuse through online and digital innovation:** ensuring that opportunities for abuse are identified and 'designed out' at the initial planning and design stages; delivering rigorous safety assessments of new products; and establishing necessary safety features where required.
    - **Establishes enforcement powers for the Secretary of State,** which would enable the Government to enforce the statutory code of practice and related minimum standards.

For more information please contact:

Lucy Hadley: Campaigns & Public Affairs Officer
Telephone: 020 7566 2517
Email: l.hadley@womensaid.org.uk

[5] NSPCC, Age Verification in the Digital Economy Bill: Public Bill Committee Evidence from the NSPCC, October 2016
[6] Law Commission, 13th Programme of Law Reform, http://www.lawcom.gov.uk/13th-programme-potential-projects/