Tackling domestic abuse in a digital age

A Recommendations Report on Online Abuse by the All-Party Parliamentary Group on Domestic Violence

February 2017
The All-Party Parliamentary Group (APPG) on Domestic Violence provides a forum for discussion on how policy and legislation relating to domestic violence is affecting survivors and specialist support services. Women’s Aid provides the Secretariat to this group and supports the group in an administrative and operational capacity. The Chair of the APPG is Jess Phillips MP, and the Vice-Chair is Maria Miller MP.

This is not an official publication of the House of Commons or the House of Lords. It has not been approved by either House or its committees. All-Party Parliamentary Groups are informal groups of Members of both Houses with a common interest in particular issues. The views expressed in this report are those of the group.

The report was researched and compiled by Women’s Aid.

Report author:
Lucy Hadley

Production and Design:
Susannah Marwood/Hannah Atkinson

Published by:
Women’s Aid Federation of England,
PO Box 3245, Bristol, BS2 2EH
© Women’s Aid 2017
The world in which domestic abuse is perpetrated is changing, but domestic abuse persists at worrying levels. Perpetrators of domestic abuse now routinely use technology and social media to control and instil fear in those they victimise. The online world is frequently used as a vehicle for coercive control, giving perpetrators more opportunities to monitor, humiliate, threaten and abuse.

The All-Party Parliamentary Group (APPG) on Domestic Violence responded to this growing threat by convening an Expert Discussion on the issue of online abuse in October 2016. Our discussions with experts achieved a clear consensus that legislation, the police and online providers, support services, and educators are currently all struggling to keep up with the rapid growth of this crime.

The APPG on Domestic Violence welcomes considerable progress made in preventing, tackling and supporting victims of domestic abuse and other forms of violence against women and girls (VAWG) in recent years. We have seen new legislation on coercive control, greater training and awareness within the police and other statutory agencies, and steps towards a more victim-centred approach to survivors of domestic abuse within the criminal justice system. But progress risks being undermined by the growing scale and severity of abuse perpetrated online.

Based on our Expert Discussion, and evidence submitted to the APPG, we have made a range of recommendations on the action needed to modernise the response to online forms of domestic abuse and violence against women and girls – which are summarised here:

1. Online abuse must be recognised by the Government, judiciary and all relevant agencies as a harmful form of domestic abuse and violence against women and girls. The crime must be sanctioned robustly, without blaming victims. Policies, strategies, training and awareness-raising on domestic abuse and coercive control by Government, statutory agencies and support services – including specialist domestic abuse services – must routinely cover the nature and impact of online abuse, and highlight the extent of the overlap between offline and online forms of the crime.
2. There is a compelling case for reviewing the legislative framework that deals with online forms of domestic abuse – to ensure it provides parity of protection between the online and offline worlds. Specifically, the Government should support the Law Commission to review the law on online communications, and strengthen the law on image-based sexual abuse (“Revenge Porn”) – including by granting victims anonymity.

3. The use of online technology to continue perpetrating abuse, coercion and control must be barred through criminal and civil measures, in the same way as these behaviours are prohibited in the ‘real world’. The Home Office must ensure that relevant restraining orders – including Non-Molestation Orders and Domestic Violence Prevention Orders – explicitly restrict online abuse and indirect contact between a perpetrator and a victim through social media. Any breach of a restraining order, including a DVPO, must be a criminal offence.

4. Improvements in the consistency of how online providers prevent, prohibit, and respond to the crime are required. We recommend that the Government convenes a cross-sectoral working group – including industry and other stakeholders – to establish guidelines for online providers in preventing and tackling gendered online abuse, and responding to domestic abuse and VAWG cases. We also call for new obligations on online providers to: publish clear and simple information – and deliver training to the police, prosecutors and the judiciary – on how their products and services work; consult with specialist services to ensure the safety risks of new products are assessed, tested, and resolved at the design stage; and work in partnership with specialist services to ensure that online support teams understand the nature and impact of these crimes, and respond to victims effectively.

5. The police are currently required to respond to a rapidly growing area of crime, with huge increases in volumes of reporting. Although police forces are often the first point of contact for victims, many state that they are not adequately equipped or resourced to tackle online abuse. It is critical that police training, resources, tools and expertise are commensurate with burgeoning levels of online abuse, so forces can deliver an effective response. Police Forces and Police and Crime Commissioners must also ensure that action to tackle online abuse is a central part of their domestic abuse and VAWG strategies, and is appropriately funded and prioritised at the local level.
6. Survivors of online abuse require dedicated and specialist support for safety and long term recovery. The Government must establish a sustainable long-term funding model for specialist services that alleviates current funding pressures, and provides security and consistency for the future. This should be delivered alongside additional support from online providers – such as technology user guides and manuals – to enable specialist services to effectively safeguard survivors.

7. Prevention must be the cornerstone of the response. We recommend that the Department for Education urgently introduce statutory sex and relationships education, covering online abuse and healthy relationships, as part of a whole school approach to tackling sexual harassment and violence against women and girls now and preventing it in the future. Empowering women and girls with digital skills is also a priority for developing their confidence to communicate freely and safely online.

We look forward to working with Government, online providers, the police and prosecutors, support services, and other partners to implement these recommendations. Together, we must modernise our response to domestic abuse and violence against women and girls.

Jess Phillips MP
Chair, APPG

Maria Millier
Vice-Chair, APPG

Polly Neate
CEO, Women’s Aid
Online abuse is generally defined as the use of the internet or any other electronic means to direct abusive, unwanted and offensive behaviour at an individual or group. As well as often being racist and homophobic in nature, online abuse is a gendered issue, disproportionately affecting women and girls. Research consistently shows that women are subjected to more bullying, abuse, hateful language and threats online than men.

Violence against women and girls (VAWG) is increasingly perpetrated online – both through specific, online crimes (such as image-based sexual abuse and ‘sextortion’) and through the use of technology to perpetrate ‘traditional’ crimes. For example, perpetrators can use technology as a vehicle to stalk and harass, behaviour which is persistent, unwanted and causes fear to victims, in what the Crown Prosecution Service (CPS) term ‘cyberstalking’.

Online abuse does not exist in the ‘virtual world’ alone. Women experiencing domestic abuse are not only abused offline, but frequently harassed, abused and stalked online by their partners or ex-partners. This online abuse and harassment usually forms part of a pattern of coercive and controlling behaviour – which can encompass physical abuse, emotional and psychological abuse, financial abuse and sexual abuse. A Women’s Aid survey of survivors of domestic abuse in 2013 found that 45% had experienced abuse online during their relationship. For 85% of survivors surveyed in 2015, this abuse was not only virtual – but perpetrated by a partner, or ex-partner, as part of a pattern also experienced offline.

Technology has delivered dangerous new mechanisms for control. Perpetrators can now use geolocation software and spyware for surveillance, monitoring and tracking a victim’s movements. Nearly a third of survivors surveyed by Women’s Aid have experienced the use of spyware or GPS locators on their phone or computer by a partner or ex-partner. Recent convictions under the new coercive control offence show that perpetrators use digital technology to monitor victims, and perpetrate insidious control through social media and online activity.

On 26 October 2016, the All-Party Parliamentary Group (APPG) on Domestic Violence convened an Expert Discussion to consider the scale and impact
Online abuse and cyber stalking can take a range of forms, including:

- Hacking into, monitoring and controlling social media (such as Facebook or Twitter) accounts;
- “Sextortion” – the use of images or videos of sexual acts to extort money or holding someone ransom for financial gain (blackmail);
- “Virtual mobbing” and “dog-piling”, which involve encouraging ‘virtual mobs’ to harass individuals and incite hatred;
- “Trolling” – sending abusive, menacing or upsetting messages or threats on social networks, email and chatrooms;
- Spreading lies or personal information about the person online;
- Creating fake accounts, hijacking and stealing online identities;
- Posting “photoshopped” images of persons on a social media platform;
- “Baiting”, or humiliating peers online, by labelling them as sexually promiscuous;
- Unwanted indirect contact with a person that may be threatening or menacing, such as posting images of that person’s children or workplace on a social media site;
- “Spamming” - where offenders send victims multiple junk email or viruses.

of online abuse. The Chair of the APPG, Jess Phillips MP, welcomed speakers – including the Law Commissioner for Criminal Law, Google’s Public Policy and Government Relations Manager, the founders of Victims of Internet Crime and Everyday Sexism, and the CEO of Women’s Aid – to set the scene, before contributions were made by parliamentarians and representatives from the police and judiciary, online providers, campaigners, academics, support services, and survivors of domestic and online abuse. This report sets out key issues raised in the Expert Discussion, and has been informed by additional information received by the APPG and existing research on the area. A full list of the speakers at the Expert Discussion, and supplementary information received by the APPG, is provided in the annexes to this report.
The nature and impact of online abuse

The APPG heard that there are widespread misconceptions about online abuse, which often mean it is downplayed and dismissed as a less serious crime than ‘real life’ abuse. Participants highlighted that terming obscene threats of serious violence and sexual offences as ‘banter’ was completely inappropriate in a context of record levels of violence against women and girls in society, and when, on average, two women every week are killed by a male partner or ex-partner in England and Wales. Contributors stated that online abuse is having a chilling and silencing impact on women, impeding both personal and political space. Women in public life are particularly targeted by misogynistic online abuse, and many are receiving regular rape and death threats. It was highlighted that the most extreme manifestation of this was the murder of Jo Cox, the Member of Parliament (MP) for Batley and Spen, in July 2016. Prior to her murder, Jo had received online abuse and harassment from extreme right wing groups – in the same form experienced by many female MPs who are outspoken on feminism or human rights. However, the APPG heard that the tragedy of Jo’s murder had not driven the change in the public perceptions of, and response to, online abuse that was required.

In cases of domestic abuse, online abuse must be responded to as an intrinsic part of the coercive control that entraps women in personal life. Coercive and controlling behaviour, which became a criminal offence in 2015, is defined as a “strategic course of oppressive conduct” which isolates, degrades and confines a victim, and systematically breaks down their self-esteem, freedom and space for action. As technology offers multiple ways to exercise control, it is no

---

“One misconception about technology-facilitated abuse is that online harassment is not real abuse – yet much of the abuse to which the victim is exposed is often tied to offline behaviours, including stalking and assault.”

Chair of the Association of Police & Crime Commissioners, Vera Baird QC

“Online abuse is clearly tied to a desire to silence women online (...) and uses the threat of offline violence to do so.”

Laura Bates, Founder of Everyday Sexism
longer necessary for a perpetrator to live with, or near, a victim in order to incite fear. Polly Neate, Chief Executive of Women’s Aid, highlighted the scale of the ‘real world’ threat; 50% of survivors of domestic abuse surveyed by Women’s Aid had received direct threats to them or someone they knew online – and around a third of these threats had been carried out ‘offline’.

Online abuse inflicts significant harm. The founder of Victims of Internet Crime (VOIC), Folami Prehaye, shared her personal experience of image-based sexual abuse (“Revenge Porn”) which had been perpetrated by a former controlling partner. These crimes have a severe and damaging impact, leaving victims feeling fearful, shamed, anxious and depressed, and the trauma they impose cannot be underestimated.

Frequently, however, the police and public response was to tell victims to ‘get offline’ by changing their phone number or online accounts. The APPG heard that this was an inadequate and “victim-blaming” response – as the predominance of the internet and social media in people’s lives is now established fact, and it is not realistic or appropriate to restrict the use of technology, particularly for young people. The Expert Discussion heard a clear call that such “victim-blaming” responses must be challenged, with the perpetrator held fully accountable – and robustly sanctioned – for these crimes.

**Recommendation**

- Online abuse must be recognised by the Government, judiciary, and all relevant agencies, as a harmful form of domestic abuse and violence against women and girls. The crime must be sanctioned robustly, without blaming victims. Policies, strategies, training and awareness-raising on domestic abuse and coercive control by the Government, criminal justice agencies and support services – including specialist domestic abuse services – must routinely cover the nature and impact of online abuse, and highlight the scale of overlap between offline and online forms of the crime.
The APPG heard that the current legislative framework for online abuse is outdated, overlaps confusingly with other forms of criminal legislation, and does not effectively tackle image-based sexual abuse ("Revenge Pornography").

**Complex and outdated legislation**

The discussion saw consensus that the current law governing “offensive online communications” is complex, in urgent need of modernisation and simplification, and inadequate for tackling the scale of online abuse. Recently introduced criminal offences and orders – such as “Revenge Pornography”, the offence of controlling or coercive behaviour in an intimate or family relationship, and the proposed Stalking Protection Order – recognise online forms of interpersonal offending. However, the APPG heard that the overwhelming body of law in this area precedes the digital age, and was not designed for the internet and social media. As a result, the law is uncertain about what is criminal, and what penalties and sanctions should be enforced. The use of numerous laws – including the Malicious Communications Act 1988, Section 127 of the Communications Act 2003, Public Order Act 1986, Protection from Harassment Act 1997 and the Contempt of Court Act 1981 – to tackle online abuse has resulted in overlapping offences, ambiguous definitions, and uncertainty about sanctions for content which is conveyed to a wide audience without consent, in cases of ‘retweeting’ and ‘reposting’.

In response to the rapidly changing nature of the crime, the CPS has continued to update legal guidance on prosecuting social media offences. The APPG heard, however, that guidance is no substitute for robust statutory provisions. Implementing the law through guidance causes problems for online providers when designing new platforms and services, for the police and prosecutors in effectively tackling these crimes, and for victims – who are unclear about their

---

“*The world has moved on from the age of poison pen letters – so should the law.*”

Professor David Ormerod QC, Law Commissioner for Criminal Law

“There is no substitute for making sure that the statutory provisions are clear.”

Maria Miller MP, Vice-Chair of the APPG on Domestic Violence
Tackling domestic abuse in a digital age

rights. The Law Commission is considering online abuse as an area for future law reform and outlined a clear rationale for taking legislative action now; there has been a tenfold increase in convictions under Part 1 of the Malicious Communications Act in the past decade, and the law in England and Wales is at risk of falling behind – as Law Commissions in Ireland and New Zealand have already developed recommendations for reform.

The APPG heard evidence that legal language describing online offences is also highly outdated and inappropriate – terms such as “grossly offensive” and “indecent” do not reflect the true nature and impact of these crimes, and result in inadequate categorisations and guidance.

Intersection with other offences

The APPG heard evidence that sanctions for online abuse intersect with existing legislation for a range of crimes. The new coercive control offence provides legal protection against online abuse, when perpetrated as part of a pattern of coercive and controlling behaviour. Guidance on the offence recognises that “monitoring a person via online communication tools or using spyware” is a common form of coercive and controlling behaviour.10

Recent convictions show how the new offence has enabled online forms of domestic abuse – such as control of a victim’s social media account - to be criminally sanctioned.11

At the end of the 2016, the Government introduced a Stalking Protection Order (SPO) – conditions for which include prohibiting perpetrators from contacting victims online. A breach of an SPO is a criminal offence, with a maximum sentence of up to five years.12 However, other relevant Protective Orders – such as Domestic Violence Protection Orders (DVPOs) or Non-Molestation Orders – do not automatically prohibit online contact through emails,

Coercive Control Convictions

Since Section 76 of the Serious Crime Act, Controlling or Coercive Behaviour in an Intimate or Family Relationship, came into force on 29 December 2015, convictions have included:

• “A man who had prevented the victim from seeing her friends and further isolated her by stopping her from using her mobile phone and controlling her social media, such as making her delete friends on Facebook.”

• “A man who rarely allowed the victim to go out alone, and when she did, would keep track of her (...) He belittled her and made her believe she only needed him, pushing her family and friends away. He checked her social media accounts and phone messages and told her what to wear as well as changing her hairstyle. He was also convicted for assault by beating.”

Crown Prosecution Service, June 2016
messages or social media. The APPG heard that although perpetrators are frequently using online technology to continue perpetrating abuse and coercive control, criminal and civil proceedings are not currently responding effectively to the scale of the problem. At present, prohibitions on online contact through a restraining order are made at a judge’s discretion. The APPG heard that all restraining orders should automatically prohibit a perpetrator from making online contact with a victim, or third party contact through social media. Polly Neate stated that Women’s Aid were calling for any breach of a DVPO to be a criminal offence, to ensure the order provides effective protection for victims and delivers a strong deterrent to perpetrators.

The APPG heard a range of views about the adequacy of legislation for tackling ‘cyber’ forms of stalking. Although some participants stated that implementing current laws is more important than further reform, it was highlighted by police representatives that legal complexities make effective prosecution of cyberstalking a challenge. There are examples of online communications where the content is not deemed “offensive”, but the volume and impact of the communications could be interpreted as stalking. Prosecuting cyberstalking is also more complex as anonymity – achieved through concealing email addresses and providers, or by using different internet servers – is easier to secure than in ‘real life.’ The APPG received evidence suggesting that changes in legislation to help prevent this anonymity are required.

Members of the APPG stressed the need to deliver a joined-up response to all forms of domestic abuse and VAWG, and ensure that online abuse is fully integrated within the established legal and policy framework for tackling these crimes – including within the devolved administrations.

Image-based sexual abuse

The Expert Discussion considered how the current legislation for image-based sexual abuse (“Revenge Pornography”) could be strengthened. The APPG heard that using the word “porn” – legally defined as an image produced “solely or principally for the purpose of sexual arousal” – for the crime is highly insulting to victims, who have been subject to distress, anxiety, and shame. The term also only covers one particular form of the
crime, which involves sharing private, sexual images for ‘revenge’. In reality, private sexual images are created and distributed without consent in a range of ways – including through ‘upskirting’ and sharing hacked images. Experts and survivors highlight that the crime should be defined as a form of sexual abuse, and that the term ‘image-based sexual abuse’ – recently developed by Professors McGlynn and Rackley – should be adopted.

The APPG also heard clear calls for victim anonymity in cases of image-based sexual abuse. In 1976 complainants of sexual offences were granted anonymity after research showed that, without it, the vast majority of victims would not report rape. The numerous internal and external barriers facing survivors of sexual violence in reporting the crime – including stigma and ‘victim-blaming’ attitudes, institutional and cultural difficulties, the fear of reprisal, and wanting to protect friends and family – are well documented. Even with anonymity, many victims of sexual violence do not report the crime. Although the CPS successfully prosecuted 206 cases of image-based sexual abuse in 2015, there were estimated to be at least 1,160 reported incidents in the same period. The disparity between reports and prosecutions indicates that – in addition to issues with police referrals to the CPS, and CPS charging decisions – victims are not currently confident or supported in pursuing prosecutions.

In Folami’s case, her name was printed in a local newspaper, with a circulation of over 30,000, when the images were still available online. This alerted thousands of people in her local area to the images, and exposed her to further shame and potential abuse. Anonymity is an important measure of protection and means of delivering justice for survivors of sexual offences – but it is not automatically granted when these crimes are perpetrated online. This is likely to mean that victims are reluctant to report offences, and support prosecutions, because the images could be circulated further – and the abuse may escalate.

The APPG further heard concerning evidence that open profit is generated from image-based sexual abuse, as websites that host such images receive

“A defendant who sent intimate photos of a woman to members of her family via Facebook and threatened to post further pictures online was sentenced to 12 weeks’ imprisonment suspended for 18 months after he pleaded guilty to an offence of disclosing private sexual images without consent.”

Crown Prosecution Service Annual Violence Against Women and Girls Report 2015-16
advertising revenues. Robust action is needed to ensure these websites are shut down, and creators and distributors effectively pursued and sanctioned.

**Recommendation**

There is a compelling case for reviewing the legislative framework that deals with online abuse, to ensure it provides parity of protection between the online and offline worlds for survivors of domestic abuse and VAWG. Specifically, we recommend that the Government:

- Supports the Law Commission to review the law on online communications, and prioritises the implementation of reforms proposed as a result of this work.

- Fully integrates online abuse within the existing policy and legal framework for domestic abuse and VAWG. The use of online technology to continue perpetrating abuse, coercion and control must be barred through criminal and civil measures, in the same way as these behaviours are prohibited in the ‘real world’. The Home Office must ensure that relevant restraining orders – including Non-Molestation Orders and Domestic Violence Prevention Orders – explicitly restrict online abuse and indirect contact between a perpetrator and a victim through social media. Any breach of a restraining order, including a DVPO, must be a criminal offence.

- Ends official use of the term “Revenge Porn”, ensures that websites profiting from the crime are shut down and effectively sanctioned, and grants anonymity to victims of image-based sexual abuse.
The role of online providers

Under EU law, digital intermediary service providers – such as online platforms, like Facebook or Twitter – are not liable for the content they hold and transmit passively. However, the APPG heard that online providers have a vital role in preventing and tackling the proliferation of abuse online. A number of best practice examples were noted, including quick and effective reporting procedures – which remove the onus on survivors to stop using social media platforms. Google's Public Policy Manager highlighted to the APPG that technology provides opportunities to pro-actively prevent, identify, and remove abuse online. She outlined mechanisms that the company's platforms had developed – such as how content could be 'flagged' for review on YouTube, and the ability of users to report sites used for image-based sexual abuse or sextortion, to ensure they are removed from Google's search results.

Many providers have developed voluntary standards for tackling online abuse. Twitter has recently launched a ‘Hateful Conduct’ framework to improve reporting and enforcement, are strengthening the capacity and expertise of their support teams to respond to online abuse, and are barring the most abusive individuals from creating new accounts. Facebook has launched ‘Community Standards’ that include policies to tackle sexual violence and exploitation, and has worked with domestic abuse organisations in other countries to develop safety guidelines for survivors.

Common, industry-wide standards exist in other areas of online safety – such as the safety framework of the ICT Coalition for Children Online, and the UK Council for Child Internet Safety’s (UKCCIS) ‘Practical Guide’ for protecting children's safety and wellbeing. However, there are currently no clear guidelines for preventing and responding to online abuse – particularly in cases where vulnerable people, such as survivors of domestic abuse, are victims. A range of inconsistencies in tackling the crime across the industry were raised with the APPG, including:

- No clear definitions or prohibitions for online abuse are used within online providers' terms and conditions and associated user guidance.
There are a range of approaches to in-built reporting functions, which are vital for enabling victims to directly report abusive content, specify it as an incident of domestic abuse, and restrict exposure to further abuse after reporting.

There are no clear guidelines for effectively preventing online abuse, such as: through safety assessments at the design stage of new products and services; prohibitions on the use of multiple accounts in cases of domestic abuse, cyberstalking, or other forms of VAWG; how default settings can be used to improve safety; and 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.

The industry does not have clear expectations in how to respond to criminal or civil proceedings for VAWG offences – including procedures for: handling, storing and sharing evidence of online abuse, which is vital for successfully prosecuting and convicting perpetrators; or the steps required by online providers when a restraining order (such as a Non-Molestation order) is imposed on a user.

The Department for Culture, Media and Sport has stated that the Government is working with online companies to make progress on a code of practice for online abuse. However, despite significant pressure for common standards in recent years, there has been limited progress in this area to date. The APPG notes that – due to the rapid pace of change within online technology and communications, and differences in scale across the industry – there are significant barriers to agreeing minimum standards in this area.

In order to deliver change, the APPG recommends that the Government – in partnership with online providers, the police, the Crown Prosecution Service and Law Commission, survivors, support services, academic experts, and organisations tackling domestic abuse and VAWG – prioritises the creation of industry guidelines for tackling online abuse. As part of the Violence Against Women and Girls Strategy 2016-2020, the Government has established an internal working group to address gendered online abuse and co-ordinate the response to online forms of VAWG. The group could be a starting point for

“Products in this country must be sold in the way that doesn’t break the law, or can’t be used to break the law.”

Maria Miller MP, Chair of the Women and Equalities Select Committee and Vice-Chair of the APPG on Domestic Violence
this cross-sectoral work. Guidelines could build on best practice established in other areas of online safety, and provide practical steps for the industry in tackling the inconsistencies outlined above.

The Expert Discussion noted that specialist training – delivered both by, and for, providers – is also vital for building an effective response to a rapidly changing crime. There were calls for online providers to provide simple user manuals, and additional training to the police, prosecutors and support services, on how their platforms and services work. In addition, the APPG heard that online providers themselves require training in how to deal with cases involving vulnerable people – such as survivors of domestic abuse. Online support teams would benefit from further, specialist, understanding on the context, nature and impact of these crimes – and the needs of victims – in order to respond effectively.

Recommendations

The role of online providers is critical. Improvements in the consistency of how online providers prevent, prohibit and respond to the crime are required:

• The Government should urgently convene a cross-sectoral working group – including industry, the police, prosecutors and other stakeholders – to establish guidelines for online providers in preventing and tackling gendered online abuse. This would build on best practice and set safety guidelines for: the design, development and safety assessments of new products; reporting functions; security settings; and location services. The guidelines should establish clear procedures for how providers handle, store and share evidence, and respond to civil and criminal proceedings, in cases of domestic abuse and VAWG.

• It is critical that online providers and companies consult with specialist services at the design stage of product development to ensure the safety risks of new products are assessed, tested, and resolved at the design stage.

• Specialist training – both by, and for, online providers – is imperative. There should be an obligation on online providers to publish clear information and user manuals – and provide training to the police, prosecutors, and the judiciary and support services – on how their products and services work. Online providers should also work in partnership with specialist domestic abuse and VAWG organisations, whose expertise will ensure that online support teams fully understand the nature and impact of these crimes, and can respond to victims effectively.
The APPG heard that concerted action is needed to improve the criminal justice response to online abuse. Police officers were said to not only lack a clear and effective legislative framework, but the necessary skills, training, tools and resources with which to enforce the law.

Greater Manchester Police reported that 58% of their staff felt unable to tackle online abuse effectively – and it is estimated that only around 7,500 police officers in England and Wales are trained to investigate digital offences. The current CPS guidelines were described as not delivering adequate support to the police in charging suspects, and police representatives whole-heartedly supported legal reform to provide greater certainty to forces tackling online crimes.

Resource and training constraints result in significant inconsistencies in law enforcement across police forces, and varying levels of protection for victims. The Expert Discussion heard that there are clear examples of good practice – with forces such as Nottinghamshire Police having recently defined misogyny as a hate crime, and Police and Crime Commissioners taking on an important local accountability role. The APPG also noted that demographic changes would drive increased understanding of the crimes, as younger officers are more comfortable operating in the ‘online world’.

Concerningly, however, there was consensus that the police are not currently equipped to effectively tackle these forms of online crime. Police representatives highlighted severe challenges faced in investigating enormous amounts of illegal online content, and the technological difficulty of extracting the information needed to build
cases and convictions. The APPG heard that the most effective response was pro-active, when the police were able to target prolific and repeat abusers. Improving training in online abuse was seen as critical for empowering officers to respond to online abuse, and should be rolled out alongside the development of specialist expertise, and investment in new technological and intelligence capacity, in this area.

Recommendation

• The police are currently required to respond to a rapidly growing area of crime, with huge increases in volumes of reporting. Although police forces are often the first point of contact for victims, many state that they are not adequately equipped or resourced to tackle online abuse. It is critical that police training, resources, tools and expertise are commensurate with burgeoning levels of online abuse, so forces can deliver an effective response. Police Forces and Police and Crime Commissioners must also ensure that action to tackle online abuse is a central part of their domestic abuse and VAWG strategies, and is appropriately funded and prioritised at the local level.
Staying safe online can be difficult, and is particularly challenging for women vulnerable as a result of domestic abuse and coercive control. The need to adequately support victims was a key issue raised during the Expert Discussion. Specialist services and practitioners have a critical role in supporting victims, raising awareness and gathering evidence and expertise, preventing further harm, and supporting long-term safety and recovery – both on and offline. The APPG on Domestic Violence has previously issued a report on the significant financial challenges facing specialist domestic abuse and sexual violence services, which are largely the result of budget reductions and damaging commissioning practices. Poor access to specialist services remains a significant concern for the APPG; Women's Aid reported to the APPG that, on just one day in 2015, 92 women and 75 children were turned away from a domestic abuse refuge because they could not be accommodated.

Specialist domestic abuse and VAWG services are vital partners in tackling online abuse, protecting victims, and meeting survivors' needs. They are centres of local and national expertise that can be drawn upon for advice and guidance on policy, legislation and best practice. Ensuring that online providers meaningfully consult with specialist services, and the organisations representing them, at the design stage of product development will be critical to mitigating the safety risks and implications of new online products and services.

The APPG also heard that services require additional support to improve their capacity and capability to respond to online forms of abuse. It was highlighted that frontline practitioners can struggle to ‘keep up’ with rapid changes in technology and the safety risks that survivors are facing. The APPG heard that simple information, ‘user guides’ and technology manuals produced by online providers – which clearly outline the features, functions and safety risks of platforms, products and services – are required to ensure that specialist services can safeguard survivors from online abuse.

**Recommendation**

- Survivors of online abuse require dedicated and specialist support for safety and long-term recovery. The Government must establish a sustainable long-term funding model for specialist services that alleviates current funding
pressures, and provides security and consistency for the future. This should be delivered alongside additional support from online providers – such as technology user guides and manuals – to enable specialist services to effectively safeguard survivors.
The Expert Discussion heard clearly that gendered online abuse is not caused by technology. These crimes are manifestations of violence against women and girls, defined by the UN as “any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation.”

VAWG does not take place in a cultural vacuum, but is rooted in structural inequalities of power between men and women, and reinforced by the sexism that women and girls face every day. These crimes therefore cannot solely be dealt with reactively by the police, criminal justice system, online providers and support services – they must be prevented across society.

Concerted action is needed to prevent online abuse, by tackling the causes of inequality and challenging the misogynist attitudes that reinforce it. The impact of online abuse and pornography on young people was highlighted as a particular concern, and the APPG heard there was an urgent need for prevention through education. The founder of Everyday Sexism explained how online abuse was becoming normalised for young people; control of mobile phone messaging, coercive pressure to send explicit photographs, and sharing of sexual images without consent were increasingly formative parts of early relationships. In the context of widely available misogynistic online pornography, there is often little recognition from young people that this is abnormal, or abusive, behaviour – and it sets a precedent for future online, and offline, abuse. Despite the scale of the problem, Girlguiding UK highlighted that less than half of girls responding to their recent Girls’ Attitudes Survey had reported ever learning about pornography, consent and relationships within school.

A month prior to the APPG discussion, the Women and Equalities Select Committee concluded an inquiry into Sexual Harassment in schools. The Committee reported that increasing access to pornography and technological advances fuel a “deeply troubling” culture of sexual harassment and violence – predominately perpetrated by boys against girls – and recommended that a whole school approach to tackling sexual harassment and violence is urgently
needed to protect young people. This must be underpinned by statutory age appropriate sex and relationships education (SRE), that is delivered by well-trained professionals and tackles online abuse, pornography, consent, and what constitutes a healthy relationship.\textsuperscript{24} The Chairs of the Parliamentary Select Committees for Education, Home Affairs, Health, and Business, Energy and Industrial Strategy have all supported the recommendation, and called on the Government to act.\textsuperscript{25}

In December 2016, the Department for Education responded to the Committee by stating that “existing statutory duties and guidance on equalities, safeguarding, curriculum and behaviour” – with updated guidance – provided adequate protection.\textsuperscript{26} The current Secretary of State for Education has, however, indicated that the Government’s position is under review.\textsuperscript{27} The APPG heard that the overwhelming body of expertise on this issue is clear – statutory, high quality, SRE is needed to keep girls safe from online abuse and VAWG now, and prevent the perpetration of these crimes in the future.

The APPG heard that technology has a vital part to play in women’s empowerment and ending violence against women and girls. Innovative solutions and technological advancements can help to tackle domestic abuse and VAWG, including by raising awareness, building evidence and improving access to support. For many survivors, online platforms are also vital for enabling access to support networks and forums where they can share experiences with other women. The APPG heard that action to develop digital skills, knowledge and capacity is critical to empower women to communicate freely and safely online, and supporting the future response to VAWG.

**Recommendation**

- Prevention must be the cornerstone of the response. We recommend that the Department for Education urgently introduce statutory sex and relationships education, covering online abuse and healthy relationships, as part of a whole school approach to tackling sexual harassment and violence against women and girls now and preventing it in the future. Empowering women and girls with digital skills is also a priority for developing their confidence to communicate freely and safely online.
Online technology has created a previously unimaginable world. The internet and social media can be an empowering force, disseminating information and enabling access to new connections, opportunities and support. But for some perpetrators, digital technology provides another way to harass, intimidate, abuse and control. As a result, we know that far too many women are living in fear every day.

The APPG has concluded that the scale and impact of online abuse risks undermining the significant progress made to tackle domestic abuse, and other forms of violence against women and girls, in recent years. Reforms are required to modernise the response across a range of areas – from effective and updated legislation, the action needed from the police and online providers, and the support provided to victims. Ultimately, the APPG believes that prevention – firstly through high quality statutory sex and relationships education – must be a priority if we are ever to tackle the proliferation of online abuse as a form of violence against women and girls.

The APPG welcomes the Government’s commitment within the VAWG Strategy to address online abuse, but considers that far greater political priority and impetus is required to tackle these crimes effectively. Establishing a cross-sectoral working group to tackle gendered online abuse, and to co-ordinate the response to online VAWG, is a priority. Such a group would provide the starting point for the recommendations outlined in this report – to develop practical guidelines for online providers, improve the capacity of the police to respond to the crime, boost the capability of specialist services to support victims, share best practice, and scale up prevention work. It is critical that online abuse is now fully recognised by all partners as a legitimate and harmful manifestation of violence against women and girls.

Without a dedicated drive by Government, and the implementation of these recommendations, the response to this form of crime by the police, prosecutors and online providers will continue to be inconsistent. Women and girls will continue to be fearful of speaking out on the issues that matter to them, and silenced online. Furthermore, too many survivors will continue to experience the devastating and insidious impact of online abuse, often as part of a campaign of coercive control by a perpetrator. The APPG calls for urgent action to modernise our response to 21st century forms of domestic abuse and violence against women and girls.
Annex A: The APPG and Expert Discussion on Online Abuse

Officers of the All-Party Parliamentary Group on Domestic Violence

- Jess Phillips MP – Chair of the APPG
- Maria Miller MP – Vice-Chair of the APPG and Chair of the Women and Equalities Select Committee
- Gavin Newlands MP
- Nusrat Ghani MP
- Sir Peter Bottomley MP
- Angela Rayner MP
- Thangam Debbonaire MP
- Fiona Mactaggart MP
- Caroline Lucas MP
- Baroness Thornton
- Vicky Foxcroft MP
- Gavin Newlands MP
- Sir Keir Starmer MP
- Peter Grant MP
- Sarah Champion MP
- Norman Lamb MP
- Baroness Hamwee
- Matthew Pennycook MP
- Flick Drummond MP

Members of the APPG also in attendance

- Liz McInnes MP
- Rebecca Harris MP

Speakers at the Expert Discussion on Online Abuse

- Professor David Ormerod QC – Law Commissioner for Criminal Law
- Folami Prehaye – Founder, Victims of Internet Crime (VOIC)
- Laura Bates – Founder, Everyday Sexism Project
- Polly Neate – CEO, Women’s Aid
- Katie O’Donovan – Public Policy and Government Relations Manager, Google
Additional evidence received by the APPG

- The Law Commission
- Victims of Internet Crime (VOIC)
- Vera Baird QC, Police and Crime Commissioner for Northumberland and Chair of the Association of Police and Crime Commissioners
- Professor Clare McGlynn, Centre for Gender Equal Media, Durham University
- Google
- Twitter
- Facebook
- Women’s Aid
References

1. Women’s Aid, Virtual World, Real Fear: Women’s Aid Report into online abuse, harassment and stalking (Bristol: 2014). Accessible online
2. The Centre for Gender Equal Media, Parliamentary Briefing - Online Abuse Parliamentary Debate: Law Reform and Funding Specialist Support Services, 6 July 2016
4. Women’s Aid, ‘Virtual World, Real Fear’, 2014
5. Women’s Aid, Online Safety, Accessible online
6. Women’s Aid, Online Safety, Accessible online
12. Home Office, Introducing a stalking protection order, 7 December 2016. Accessible online
13. Section 63, Criminal Justice and Immigration Act 2008
20 Hansard, Volume 612, c1069
22 Women’s Aid, Annual Survey 2015: The Results, 2016. Accessible online
23 A/RES/48/104, United Nations Declaration on the Elimination of Violence Against Women
25 Chairs’ letter to the Secretary of State regarding the status of PSHE. Accessible online
26 Government response to the Committee’s Third Report of Session 2016–17. Accessible online
27 Justine Greening MP, 14 September 2016, Education Committee – Oral evidence: Roles and Responsibilities of the Secretary of State for Education, HC196