HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 07967, 13 September 2017

Online harassment and cyber bullying

By Pat Strickland
Jack Dent

Contents:

Contents

Summary

What is online harassment?

Online harassment and cyber bullying can take a wide variety of forms including:

- "trolling" (sending menacing or upsetting messages)
- identity theft
- "doxxing" (making available personal information)
- cyber stalking

It can affect adults and children. Some argue that online bullying amongst school children is more pervasive than face to face bullying, because it can follow a child home after school, and from one school to another. The problem of online abuse of Members of Parliament has also been highlighted in recent months, particularly of female and ethnic minority MPs.

The current law

The general legal principle is that what is illegal offline is also illegal online. There are a number of criminal offences which can be involved, including stalking, harassment, sending malicious communications and improper use of a public electronic communications network. A more recent addition is the offence of "revenge pornography" under the Criminal Justice and Courts Act 2015.

The Crown Prosecution Service has published Guidelines on prosecuting cases involving communications sent via social media setting out when it will usually be in the public interest to prosecute certain types of potentially criminal communications. When section 103 of the Digital Economy Act 2017 comes into force, it will require the Government to issue guidance on action which might be appropriate for social media providers to take against bullying, intimidation or insulting behaviour.

Pressure for change

Some have argued that existing offences are adequate to deal with online harassment. Others have pointed out that several offences pre-date the widespread use of social media platforms, and have called for the law to be reviewed.

Generally recent governments have tended to favour self-regulation wherever possible, working with the industry to deal with problems that arise. There has been resistance to introducing specific legislation to deal with online harassment and trolling. However, over the past year, arguments for a change in the law seem to have been gaining ground. The Law Commission has consulted on whether it should look at the "scope and interrelationship" of the various pieces of criminal law which apply.

Will there be a change in the law?

Before the 2017 General Election was announced, the Conservative government announced that ministers had started work on a new

Internet Safety Strategy which would lead to a Green Paper in summer 2017.

The 2017 Conservative manifesto promised to take steps to protect the vulnerable online, and develop a "digital charter" balancing freedom with protection for users. This would be underpinned by a regulatory framework, with a regulator and a sanctions regime, and a power to introduce a levy from social media companies and communication service providers to counter internet harms.

The 2017 Labour manifesto promised to give the police more resources to deal with cybercrime and to ensure that "tech companies are obliged to take measures" to tackle online abuse. The Liberal Democrats promised a digital bill of rights protecting people's powers over their own information.

What can victims do?

Victims of online harassment and abuse can report this either to the police, the social media platform or both. Social media providers offer various ways of reporting abuse. Generally speaking, they tend to rely on users to make such reports, and then refer complaints to moderators who decide whether content should be removed.

Are social media companies doing enough?

The Home Affairs Committee published a report on Hate Crime in May 2017 which criticised social media and technology companies for not doing enough. Facebook announced in the same month that it would appoint an additional 3,000 content moderators to remove content more quickly in the wake of broadcasts of killings and assaults. The sheer volume of users makes the task of monitoring content very difficult.

Scotland

Scotland also has a range of offences which can be used to deal with online and offline abuse. These include threatening and abusive behaviour, stalking and improper use of a public telecommunications network, along with common law offences such as breach of the peace. The Protection from Harassment Act 1997 provides civil remedies in Scotland. Scotland has also introduced a new offence to deal with "revenge pornography".

Northern Ireland

Northern Ireland has its own Protection from Harassment (Northern Ireland) Order, and Malicious Communications (Northern Ireland) Order. Like England, Scotland and Wales, it is covered by the provisions in the Communications Act 2003 which make it an offence to make improper use of a public communications network.

Further information

More detailed information on the law on harassment is available in Library Briefing Paper 6648, The Protection from Harassment Act 1997.

Library Briefing Paper 6261, Stalking: Criminal Offences looks at the specific stalking offences which have been introduced in England and Wales and in Scotland.

1. The problem

Online harassment and cyber bullying can take a variety of forms, and can affect children and adults. The Stop Online Abuse website which provides advice to people affected by offensive or damaging online content, lists examples of online harassment or abuse:

- trolling
- trying to damage your reputation by making false comments
- accusing you of things you haven't done
- tricking other people into threatening you
- stealing your identity
- setting up profiles in your name
- electronic sabotage
- publishing personal information about you, sometimes called doxxing (including sex videos and photos, which is sometimes called 'revenge porn')
- cyber-stalking
- encouraging other people to be abusive or violent towards groups of people.

The National Society for the Prevention of Cruelty to Children (NSPCC) says that cyberbullying is an increasingly common amongst children and lists similar examples of what constitutes online abuse:

- sending threatening or abusive text messages
- creating and sharing embarrassing images or videos
- 'trolling' - sending of menacing or upsetting messages on social networks, chat rooms or online games
- excluding children from online games, activities or friendship groups
- setting up hate sites or groups about a particular child
- encouraging young people to self-harm
- voting for or against someone in an abusive poll
- creating fake accounts, hijacking or stealing online identities to embarrass a young person or cause trouble using their name
- sending explicit messages, also known as sexting
- pressuring children into sending sexual images or engaging in sexual conversations[1]

[1] NSPCC website, Bullying and cyberbullying: what are bullying and cyberbullying?, accessed 31 May 2017; see also BullyingUK website, What is cyber bullying?, accessed 31 may 2017

2. Recent governments' approaches to internet regulation

Previous governments have tended to favour self-regulation and working with stakeholders rather than regulating internet content.

Generally, recent governments have tended to favour self-regulation wherever possible and take what is often called a "multi-stakeholder approach" to internet regulation.[2] This means working work with business, industry groups, civil society and other governments to deal with issues which arise. The broad approach has been to put in place a legal framework for specific issues rather than regulate the internet or internet content. This approach was summed up in a reply to a Parliamentary Question in 2013 by Lord Gardiner of Kimble (then Lords spokesperson on Culture, Media and Sport for the Coalition government):

> Government favours a self-regulatory approach to the internet; it is not for Government to tell media organisations whether they can publish certain content, beyond that which is illegal.[3]

In a July 2016 debate on online abuse, Ed Vaisey (then Minister of State for Culture and the Digital Economy), also emphasised this multi-stakeholder, self-regulatory approach:

> The UK has led the way in approaching the issue from a perspective of self-regulation rather than legislation. Self-regulation works because it brings about partnerships and helps us to move forward more quickly. A good example is the creation of the Internet Watch Foundation, which was the first charity to focus on dealing with images of child sexual abuse. It is a model that has been copied around the world, and it became incredibly important in driving forward the recent work with search engines, such as Google, to make searching for and discovering images of child abuse online much, much more difficult. We have worked with the Internet Watch Foundation to ensure that internet service providers had the funding to increase their capacity, and we have worked with technology providers on the use of technology that enables images to be matched and traced, and that makes it easier to catch and trace perpetrators. [4]

However, the Conservative manifesto said that a Conservative government would not only develop a digital charter, to "balance freedom with protection for users" but would also create a "regulatory framework in law" to underpin this.[5] The Labour manifesto promised to ensure that "tech companies are obliged to make measures" to tackle online abuse. [6] Further detail is in section 5.3, below.

---

2 See, for example, HC Deb 11 Nov 2013 c471W and UK Government, *A safe and secure cyberspace - making the UK the safest place in the world to live and work online*, Policy Paper 5 in the *UK Digital Strategy* , 1 March 2017

3 HL Deb 21 November 2013, cWA231

4 HL Deb 7 July 2016 c1104

5 Conservative and Unionist Party, Forward Together Our Plan of a Stronger Britain and a Prosperous Future, p83

6 Labour Party, For the many not the few: The Labour manifesto 2017, p96

3. The law in England and Wales

3.1 Relevant offences

The general legal principle is that what is illegal offline is also illegal online.

Successive governments have repeated the general legal principle that what is illegal offline is also illegal online. [7] Rather than specific offences of, for example, cyberbullying or online harassment, there a number of existing offences can apply to various kinds of online abuse.

These include:

- stalking and "stalking involving fear of violence or serious alarm or distress" - sections 2A and 4A of the Protection from Harassment Act 1997 (as amended)
- harassment - section 2 of the Protection from Harassment Act 1997
- improper use of a public electronic communications network - section 127 of the Communications Act 2003
- sending indecent, grossly offensive, false or threatening communications - section 1 of the Malicious Communications Act 1988

A new offence of revenge pornography covers "the sharing of private, sexual materials, either photos or videos, of another person, without their consent and with the purpose of causing embarrassment or distress". It was introduced by section 33 of the Criminal Justice and Courts Act 2015.[8]

The offence applies equally online and offline and to images which are shared by electronic means or in a more traditional way. The Crown Prosecution Service (CPS) has published guidance specifically on prosecuting cases involving revenge pornography.[9]

3.2 Guidance on prosecuting social media offences

The CPS has also published broader guidance, Guidelines on prosecuting cases involving communications sent via social media. The guidance divides potentially criminal communications into four categories. The first three are those which may:

- constitute threats of violence to the person or damage to property

---

7 See, for example, HC Deb 29 October 2013 c236-7WA; Culture Media and Sport Committee, Online Safety: Responses to Committee's Sixth Report of Session 2013-14, 3 July 2014, HC 517 2014-15, page 11; PQ 224106 and PQ 224105, both answered 23 February 2015

8 Ministry of Justice (MoJ), *Revenge porn: the facts*, February 2015; MoJ, "New law to tackle revenge porn", 12 October 2014

9 CPS, *Revenge Pornography - Guidelines on prosecuting the offence of disclosing private sexual photographs and films*, March 2016

- specifically target individuals, for example involving harassment, stalking, controlling or coercive behaviour, “revenge pornography” or sexual offences
- breach a court order or statutory prohibition

The fourth category is:

- “Communications which do not fall into any of the categories above fall to be considered separately i.e. those which may be considered grossly offensive, indecent, obscene or false.”

The guidance says that, while it will usually be in the public interest to prosecute cases in the first three categories (providing they satisfy the normal evidential test), cases in the fourth category “will be subject to a high evidential threshold and in many cases a prosecution is unlikely to be in the public interest.”

CPS guidance sets out when it will normally be in the public interest to prosecute potentially criminal communications.

An accompanying press release set out some of the new issues covered by the revised guidelines such as:

- encouraging others to participate in online harassment campaigns (“virtual mobbing”)
- making available personal information, for example a home address or bank details – ("doxxing")
- creating a derogatory hashtag to encourage harassment of victims
- cyber-enabled Violence against Women and Girls and hate crime offences, such as include 'baiting', the practice of humiliating a person online by labelling them as sexually promiscuous or posting 'photoshopped' images of people on social media platforms.

The press release also describes the guidance on “sexting” making it clear that it would not normally be in the public interest to prosecute consensual sharing between children of similar ages in a relationship:

> The guidance provides information for prosecutors considering cases of 'sexting' that involve images taken of under-18-year-olds. It advises that it would not usually be in the public interest to prosecute the consensual sharing of an image between two children of a similar age in a relationship. A prosecution may be appropriate in other scenarios, however, such as those involving exploitation, grooming or bullying.[10]

[10] Crown Prosecution Service, CPS publishes new social media guidance and launches Hate Crime consultation, 10 October 2016

3.3 A new code of practice

Section 103 of the Digital Economy Act 2017 will, when it comes into force, require the Secretary of State to issue guidance to the providers of online social media about action it might be appropriate to take against:

- bullying or insulting behaviour
- behaviour likely to intimidate or humiliate an individual.

The Conservative government added this to the Digital Economy Bill during the final stages ("Ping Pong")[11] to replace an Opposition amendment which had been agreed to in the Lords.[12] However, unlike the Opposition amendment it replaced, section 103 does not contain a requirement for social media providers to follow the guidance.

The Digital Economy Act 2017 will require the Government to issue guidance on action against online bullying, intimidation or humiliation.

11 HC Deb 26 April 2017 c1124; HL Deb 27 April 2017 cc1491-1493
12 Lords Amendment 40

4. Do we need specific law for online harassment?

There have been calls for changes to legislation, consolidation of the law or improved guidance.

Some of the laws used to prosecute online harassment predate the widespread use of the internet and social media. Some people have called for a coherent, unified body of law aimed specifically at online activities. In recent years, a number of parliamentary select committees have investigated this question, and come to different conclusions.

In March 2014, the Culture, Media and Sport Committee published a report on online safety which suggested that the law might need to be clearer on the status of bullying:

> Any changes to legislation, including consolidation of current laws, which clarify the status of bullying, whether off-line or online, would be welcome. At the same time, much could be achieved by the timely introduction of improved guidance on the interpretation of existing laws.[13]

The Coalition government rejected the suggestion that clarification or consolidation was necessary:

> It is of course the case that what is illegal offline, is illegal online. As the Committee notes, there is a wide range of offences that could cover bullying behaviour depending on the nature of it and the circumstances under which it takes place.
>
> These laws are effective and are well understood by practitioners and the police and appropriately interpreted and enforced by the courts in relation to both on-line and off-line conduct. As things stand, the Government is not aware of any evidence to suggest the need for further clarification in this area and whilst the laws are kept under constant review, the Government has no current plans to consolidate them.[14]

In February 2016, in answer to a Parliamentary Question, the Conservative government rejected the idea of making bullying a criminal offence:

> We do not want to make any form of bullying a criminal offence as to do so would risk criminalising young people. In some circumstances that may be justified, but probably only in a limited number of very serious cases, for which there are already laws in place to protect people. Internet providers, schools and parents all have a role to play in keeping children and young people safe online.[15]

In July 2014, the House of Lords Communications Committee published a report on Social media and criminal offences which concluded that although much of the relevant law predated social media, it was still "generally appropriate":

---

13 Culture Media and Sport Committee, Online Safety, 13 March 2014, HC 729 2013-14, para 97

14 Culture Media and Sport Committee, Online safety: Responses to the Committee's Sixth Report of Session 2013–14, 3 July 2014, HC 517 2014-15

15 PQ 27104 [on Internet: Bullying] answered 23 February 2016

> Our overall conclusion is that the criminal law in this area, almost entirely enacted before the invention of social media, is generally appropriate for the prosecution of offences committed using the social media.[16]

Some have argued that the existing laws are adequate to prosecute online harassment and bullying.

While the Committee proposed some changes to the law, it was not persuaded that a new set of offences was necessary, and that the current range offences, "notably those found in the Protection from Harassment Act 1997 was "sufficient to prosecute bullying conducted using social media".[17] The same principle applied to "trolling":

> Similarly, sending a communication which is grossly offensive and has the purpose of causing distress or anxiety is an offence under section 1 of the Malicious Communications Act 1988. Although we understand that "trolling" causes offence, we do not see a need to create a specific and more severely punished offence for this behaviour.[18]

Others have called for a review of the whole legislative framework.

By contrast the Home Affairs Select Committee's April 2017 report on hate crime called for the Government to review the entire legislative framework governing online hate speech, harassment and extremism:

> Most legal provisions in this field predate the era of mass social media use and some predate the internet itself. The Government should review the entire legislative framework governing online hate speech, harassment and extremism and ensure that the law is up to date. It is essential that the principles of free speech and open public debate in democracy are maintained—but protecting democracy also means ensuring that some voices are not drowned out by harassment and persecution, by the promotion of violence against particular groups, or by terrorism and extremism.[19]

In December 2015, Labour's Yvette Cooper (who was Chair of the Home Affairs Select Committee when that report was published) launched Recl@im the Internet[20] which describes itself as a "broad based campaign for action to challenge abuse online".

16 House of Lords Communications Committee, Social media and criminal offences, 29 July 2014, HL 37 2014-15, para 15
17 Ibid, para 32
18 Ibid
19 Home Affairs Committee, Hate crime: abuse, hate and extremism online, 1 May 2017, HC 609 2016-17, para 56
20 "Yvette Cooper launches 'Reclaim the Internet' campaign to stop online sexism", *Politics Home*, 17 December 2015

5. Will there be changes to the law?

In February 2016, the Conservative government said that it did not intend to introduce specific additional legislation to address online harassment and internet trolling, because the existing legislation was sufficient.[21]

Over the past year, the arguments for a change in the law seem to have been gaining ground.

However, more recently, in the July 2016 debate on online abuse cited in section 1 of this Briefing Paper above, there were calls for specific laws to tackle online abuse. In response, the Minister Ed Vaisey acknowledged the "clear call from the House for legislative clarity, both clarity in defining online abuse and clarity about the myriad different Acts and statutes that come to bear in this area".[22]

5.1 The Law Commission consultation

In July 2016, the Law Commission launched a public consultation on whether reform of the law on online communications should be part of its 13th Programme of Law Reform. The Commission noted that the "the criminal law seeks to tackle offensive internet communications through a number of legislative provisions, many of which precede the digital age and vast growth in the use of social media." [23] It said that the "scope and interrelationship" between these laws is "unclear":

The Law Commission has consulted on whether it should look at the scope and interrelationship of the current laws in 2017.

> For example, Part 1 of the Malicious Communications Act 1988 makes it an offence to send a communication which is "indecent or grossly offensive" with the intention of causing "distress or anxiety"; and section 127 of the Communications Act 2003 applies to threats and statements known to be false, but also contains areas of overlap with the 1988 Act. 1209 people were convicted under section 127 in 2014, (compared to 143 people in 2004). Part 1 of the Malicious Communications Act saw a ten-fold increase in the number of convictions over the same period.
>
> (…)
>
> In addition to the 1988 and 2003 Acts, online abuse may be caught by several other provisions. The scope and inter-relationship between these provisions (covering, among other things, harassment, public order offences and revenge porn) is unclear. There is a clear public interest in tackling online abuse and "trolling", but this must be done through clear, and predictable legal provisions.
>
> The Law Commission could consider whether the current law is capable of dealing with offensive internet communications, and whether there is scope for simplifying the law in this difficult area.[24]

The closing date for the public to send their submissions was 31 October 2016. The Law Commission had originally intend to present a draft programme to the Lord Chancellor in June 2017, with a view to laying it before Parliament, but the election meant that was

21 PQ 25115 (on Internet Bullying), answered 4 February 2016
22 HC Deb 7 July 2016 c1106
23 Law Commission, Online Communications, July 2016
24 Ibid

no longer possible. It is now expected a draft programme will be presented to the Lord Chancellor soon after the Summer recess.[25]

5.2 A Green Paper in 2017?

In February 2017 the Government announced that it was working on a new internet safety strategy.

Before the 2017 General Election was called, the Conservative government announced that ministers had "begun work on a new Internet Safety Strategy"[26] and that a Green Paper on online safety would be published in summer 2017. The work, to focus on children and young people, was expected to centre on four main priorities:

- how to help young people help themselves
- helping parents face up the dangers and discuss them with children
- industry's responsibilities to society
- how technology can help provide solutions

The press release did not mention changes to legislation, but it did state the Government's ambition for the "UK to be safest place in the world for young people to go online.[27]

5.3 The 2017 General Election manifestos

A number of General Election manifestos covered the issues of internet regulation and online safety.

Conservative

The 2017 Conservative Manifesto promised a digital charter underpinned by a regulatory framework and a sanctions regime.

The 2017 Conservative Party manifesto repeated the ambition that the UK should be "the safest place to be online":

> In harnessing the digital revolution, we must take steps to protect the vulnerable and give people confidence to use the internet without fear of abuse, criminality or exposure to horrific content. Our starting point is that online rules should reflect those that govern our lives offline. It should be as unacceptable to bully online as it is in the playground, as difficult to groom a young child on the internet as it is in a community, as hard for children to access violent and degrading pornography online as it is in the high street, and as difficult to commit a crime digitally as it is physically.[28]

A Conservative government would develop a "digital charter" to "establish a new framework that balances freedom with protection for users". However, it would also establish a "regulatory framework in law" to underpin this:

> **Some people say that it is not for government to regulate when it comes to technology and the internet.** We disagree. While we cannot create this framework alone, it is for government, not private companies, to protect the security of people and ensure the fairness of the rules by which people

25 Law Commission, *13th Programme update*, 9 May 2017
26 DCMS, Government launches major new drive on internet safety, 27 February 2017
27 Ibid
28 Conservative and Unionist Party, Forward Together Our Plan of a Stronger Britain and a Prosperous Future, p79

> and businesses abide. Nor do we agree that the risks of such an approach outweigh the potential benefits. It is in the interests of stable markets that consumers are protected from abusive behaviour, that money is able to flow freely and securely, and that competition between businesses takes place on a level playing field. It is in no-one's interest for the foundations of strong societies and stable democracies – the rule of law, privacy and security – to be undermined.
>
> So we will establish a regulatory framework in law to underpin our digital charter and to ensure that digital companies, social media platforms and content providers abide by these principles. We will introduce a sanctions regime to ensure compliance, giving regulators the ability to fine or prosecute those companies that fail in their legal duties, and to order the removal of content where it clearly breaches UK law. We will also create a power in law for government to introduce an industry-wide levy from social media companies and communication service providers to support awareness and preventative activity to counter internet harms, just as is already the case with the gambling industry.[29]

The manifesto said the Government would work with industry to introduce new protections for children, and would:

> make clear the responsibility of platforms to enable the reporting of inappropriate, bullying, harmful or illegal content, with take-down on a comply-or-explain basis.

In addition:

- relationships and sex education in primary and secondary schools would team about risks including cyberbullying and online grooming
- there would be new data protection rights "including the ability to require major social media platforms to delete information held about them at the age of 18"
- there would be a new "expert Data Use and Ethics Commission to advise regulators and parliament on the nature of data use and how best to prevent its abuse."[30]

Labour

The Labour manifesto promised to give the police "the equipment and people they need to provide effective policing services, including from the growing threat of cybercrime."[31] It highlighted the issue of children's online safety:

> We all need to work harder to keep children safe online. Labour will ensure that tech companies are obliged to take measures that further protect children and tackle online abuse. We will ensure that young people understand and are able to easily remove any content they shared on the internet before they turned 18.[32]

Liberal Democrat

---

29 Ibid, p83
30 Ibid
31 Labour Party, For the many not the few: The Labour manifesto 2017, p76
32 Ibid, p96

The Liberal Democrat manifesto said the party would:

> Introduce a digital bill of rights that protects people's powers over their own information, supports individuals over large corporations, and preserves the neutrality of the internet.[33]

Green Party

The Green Party manifesto said more generally that "fairness matters online and in the media too" and that "the internet should be free of state and corporate surveillance, with our rights and freedoms protected."[34]

UKIP

UKIP's manifesto said the party would "extend the remit of the current cross-government Internet Safety Strategy and invite participants to consider whether new legislation is required to address the problem of online abuse."[35]

---

33 Liberal Democrat Party, Change Britain's future: Liberal Democrat Manifesto 2017, p72
34 Green Party, The Green Party for a Confident and Caring Britain, 2017, p21
35 UK Independence Party, Britain Together: UKIP 2017 Manifesto, p22

6. Children and online bullying

As children spend significant amounts of time online, bullying which would once have been confined to the playground and the street can spread to their online lives. A 2017 House of Lords Communications Committee report pointed out how pervasive the problem can be:

> While it used to be the case that school bullying stopped when a child went home for the day, online bullying can go on ceaselessly. It can follow a child from one school to another. It also lacks face to face interaction, so a child may not see the harmful impact of what they are saying or doing upon another child.
>
> (…)
>
> Bullying does not have to be targeted at individual children to have a negative effect. A 2014 Girls' Attitudes Survey found that "45% of those aged 13 to 21 say that they have heard about sexist abuse of women in the media on social media channels and 49% say that this restricts what they do or aspire to in some way".
>
> The 'always on' culture also has an impact on those children who may be victims of bullying. Nicola Blackwood MP, the Parliamentary Under-Secretary of State for Public Health and Innovation at the Department for Health, told the Committee: "It used to be that if you were bullied in one school you could leave, go to another school and leave it behind. You cannot really do that now." This inability to "shut out" their harassers can have an extremely detrimental impact on a young person's mental health and wellbeing. [36]

The Committee concluded that the current regime of self-regulation was underperforming and that it would "take a step change from the highest level of the Government to represent the needs of children online".[37]

In April 2017, the NSPCC published its Net Aware guide. The press release accompanying the report said that the research informing it showed that four out of five children felt social media companies weren't doing enough to protect them:

> Out of 1,696 children and young people who took part in our Net Aware research, 1,380 thought social media sites needed to do more to protect them from inappropriate or harmful content.
>
> When asked about what they were coming across on social media sites, children reported seeing:
>
> - pornography
> - self-harm
> - bullying and hatred.[38]

---

36 Lords Select Committee on Communications, Growing up with the internet, 21 March 2017, HL 130 2016-17, paras 116-118
37 Ibid, para 352
38 NSPCC, Social media sites failing to protect children, April 2017

A 2016 NSPCC report on child safety in the UK found that in 2015/16 there were:

- 4,541 Childline counselling sessions where cyber bullying was mentioned - a 13% increase since 2014/15
- 1,392 Childline counselling sessions where sexting was mentioned – a 15% increase since 2014/15[39]

A 2014 NSPCC study found that 28% of 11-16 year olds on social networking sites had experienced something that had upset them. Other findings included that:

- The most common upsetting experiences were trolling (experienced by 37% of those who had had an upsetting experience), feeling excluded from a social group or friendship (22%), aggressive or violent language (18%) and pressure into looking or acting a certain way (14%)
- 11% of these children experienced upsetting experiences every day or almost every day, and 26% at least once or twice a week
- 45% of upsetting experiences were one-off events, but 8% lasted over a month, with 3% lasting over three months
- 36% of these children got over the experience straight away or within a day, but 5% were upset for "a few" or "many" months afterwards, and 4% are yet to get over the experiences
- Although more girls had experienced something upsetting in the past year (32% compared to 24%), a higher proportion of boys than girls experienced these every day or almost every day (16% compared to 8%)[40]

What can parents do?

Ofcom research, published in January 2014, found that over half of parents did not use parental controls. The main reasons were a combination of trusting or supervising the child (depending on their age) but a lack of awareness and understanding was also a key reason.[41]

In 2016, the Department of Culture and Sport provided guidance on child online safety for social media providers.[42] This includes a summary of actions they should take to prevent and deal with

- Explain to users the type of behaviour you do and don't allow on your service.
- Make it easy for users to report problem content to you.
- Create a triage system to deal with content reports.

---

39 Holly Bentley et al, *How safe are our children? The most comprehensive overview of child protection in the UK*, NSPCC, 2016

40 Claire Lilley, Ruth Ball and Heather Vernon, The experiences of 11-16 year olds on social networking sites, NSPCC, 2014

41 Ofcom, *Report on Internet safety measures Strategies of parental protection for children online*, January 2014, pp506

42 DCMS, *Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services*, March 2016

- Work with experts to give users additional information and local support.
- For under-13s, talk in their language, and pre- and post-moderate their content.[43]

[43] Ibid, p3

7. Online abuse of Members of Parliament

In January 2017, the BBC reported the results of a survey which, it said, showed that an "overwhelming majority" of women MPs have received online and verbal abuse from the public, and a third had considered quitting as a result.[44]

A BBC survey showed widespread abuse of women MPs.

A Written Answer to a Parliamentary Question in the same month stated January 2017, reproduced below, includes the statement that:

> Members are encouraged to report all social media abuse and threats to the Parliamentary Liaison and Investigation Team (PLAIT), based in Westminster. This police unit provides support to individual Members about security concerns and co-ordinates the response with local forces.
>
> The House has a policy of not commenting publicly on specific security matters. However, the Parliamentary Security Director is happy to meet the right hon. Member to discuss the level of online abuse of female hon. Members.
>
> The Parliamentary Security Department, in conjunction with the police digital crime unit and social media companies, have run workshops for Members on this issue and provides general security advice on social media harassment[45]

An earlier survey by the Inter Parliamentary Union, based on a small sample of just 55 MPs from parliaments all over the world, suggested that sexual harassment of female MPs could be a widespread problem. Over 80% said they had experienced some form of psychological or sexual harassment or violence.[46]

There is some evidence that this may be a global problem.

The Home Affairs Select Committee's April 2017 report on hate crime also highlighted the problem:

> 17. Members of Parliament have also experienced high levels of racism, misogynistic abuse and other forms of harassment on Twitter. Rt Hon Lindsay Hoyle MP, the principal Deputy Speaker, told us that all MPs were vulnerable to abuse, but that it particularly affected women MPs, and that it was possible to "break that down even further to ethnic minority MPs and, in particular, ethnic minority women MPs".
>
> 18 Diane Abbott MP has spoken out about her experiences of receiving racist and sexist abuse online on a daily basis. She said: I have had rape threats, death threats, and am referred to routinely as a bitch and/or nigger, and am sent horrible images on Twitter. The death threats included an EDL-affiliated account with the tag "burn Diane Abbott".
>
> 19 Our October 2016 report on Antisemitism in the UK included a number of examples of deeply antisemitic tweets that were directed at Luciana Berger MP.
>
> 20 Other women MPs have also spoken out bravely about the abuse they have received just for being women in the public

The Home Affairs Committee highlighted racist, sexist and anti-Semitic abuse of MPs on Twitter.

44 "Mistreatment of women MPs revealed", BBC News, 25 January 2017
45 PQ 61644 [on Members: Harassment] answered on 30 January 2017
46 "Sexual harassment of female MPs widespread, report says", BBC News, 26 October 2016

eye, including Caroline Ansell MP and Anna Soubry MP; and Tulip Siddiq MP and Jess Phillips MP, who have had huge numbers of death and rape threats targeted at them in recent months. [47]

2017 General Election

In the recent general election campaign, candidates from all parties reported increased abuse and intimidation. Following complaints from MPs, the Prime Minister held a cabinet discussion on 4 July about their concerns.[48] In a Westminster Hall debate on 12 July on the abuse and intimidation of candidates and the public in UK elections, Members from several parties spoke about high levels of online abuse.[49]

Parliamentary candidates in the recent general election reported high levels of online abuse.

Research conducted by the University of Sheffield and BuzzFeed News in July 2017 analysed 840,000 abusive tweets made in the run-up to the general election.[50] The research found that more than 50% of the total number of abusive tweets in the run-up to the election targeted Jeremy Corbyn, Theresa May, Boris Johnson and Sadiq Khan. The top 10 most-targeted individuals accounted for over 70% of all abusive tweets.

Prominent politicians accounted for the majority of abuse. Male Conservative candidates received the highest percentage of abuse on

When broken down by party and gender, male Conservative candidates received the highest percentage of abuse in their mentions, at almost 6%. The research noted that this might be explained by more prominent politicians being male than female, and because the UK was governed by a Conservative majority before the election.[51]

Independent review into abuse of Parliamentary candidates

During the Westminster Hall debate, Chris Skidmore, the Minister for the Constitution, announced a review into the issue of intimidation experienced by Parliamentary candidates.[52] The Committee on Standards in Public Life (CSPL) will look at the nature of the problem, consider current protections and measures in place, and then report back to the Prime Minister with recommendations.[53] The report will consider both offline and online abuse.

The Committee on Standards in Public Life is conducting a review into abuse of Parliamentary candidates.

A consultation ran from 24 July to 8 September, and CSPL is currently analysing submissions.[54]

---

47 Home Affairs Committee, Hate crime: abuse, hate and extremism online, 1 May 2017, HC 609 2016-17, paras 17-20
48 'No 10 to investigate abuse of candidates in election campaign', *Guardian*, 4 July 2017
49 HC Deb 12 July 2017 cc152-70WH
50 University of Sheffield, *University of Sheffield research shows MP Twitter abuse double after terror attacks*, 25 July 2017
51 'This is what the Twitter abuse of politicians during the election really looked like,' *BuzzFeed News*, 23 July 2017
52 HC Deb 12 July 2017 c166WH
53 Cabinet Office Press release, Review into abuse and intimidation in elections, 12 July 2017
54 Committee of Standards in Public Life, Intimidation of Parliamentary candidates: CSPL Call for Evidence, 24 July 2017

8. Reporting online abuse and harassment

People who suffer online abuse or harassment can report it to the police and/or to the social media platform.

People can report online abuse to the police and/or to the social media platform.

The Crown Prosecution Service's Guidelines on prosecuting cases involving communications sent via social media gives an overview of what people suffering abuse can do:

> A number of platforms have developed tools to make reporting easier, to secure potential evidence and to prevent unwanted communications, including those that do not amount to a criminal offence. These include:
>
> - A report link, so that particular or multiple communications can be reported directly to the platform. Social media sites may then decide to remove content and disable or suspend accounts, although it is not technically possible for a platform to guarantee a user will not return once their account is closed. Note that if a matter is reported to the police, the police should make a data retention request to the platform, so that evidence is secured for any investigation.
> - Taking screenshots of the offending material, which can be saved on or off (for example, cloud storage or a USB drive) the device.
> - Tools to block or mute the person who has uploaded abusive content, so that they can no longer see posts or have a conversation with the victim.
> - Tools to unsubscribe or "un-follow" accounts that produce or share offensive material.
> - Login alerts, which prompt the platform provider to send a notification if someone tries to log into an account from a new place.
> - Privacy settings, to control who can see posts and information from profiles, such as phone numbers and email address.

8.1 What are social media companies doing?

Facebook, Microsoft, Twitter and YouTube have agreed a Code of Conduct on Countering Illegal Hate Speech Online with the European Commission.[55] This states that these companies will:

- take the lead "in countering the spread of illegal hate speech online"
- have "clear and effective processes to review notifications regarding illegal hate speech
- share best practice with other internet companies, platforms and social media companies,.

[55] European Commission, Countering illegal hate speech online #NoPlace4Hate, 4 April 2017

Facebook has sections on Staying Safe, Reporting Abuse and bullying and harassment:

> Facebook offers these tools to help you deal with bullying and harassment. Depending on the seriousness of the situation:
>
> Unfriend the person. Only your Facebook friends can contact you through Facebook chat or post on your Timeline.
>
> Block the person. This will prevent the person from adding you as a friend and viewing things you share on your Timeline.
>
> Report the person or any abusive things they post.
>
> The best protection against bullying is to learn how to recognize it and how to stop it. Here are some tips:
>
> **Don't retaliate.** Most bullies are looking for a reaction, so don't give them one.
>
> **Don't keep it a secret.** Reach out to someone you trust, like a close friend, family member, counselor or teacher, who can give you the help and support you need.
>
> **Document and save.** If someone has posted something you don't like, you can print or take a screenshot of it in case you need to share it with someone you trust later.
>
> If you feel you're in immediate danger, contact your local authorities.

There is also a Bullying Prevention Hub.

Twitter's rules state that those engaging in violent threats, harassment or hateful conduct may have their accounts temporarily locked and/or subject to permanent suspension. There is a section online abuse:

> **When to report it?**
>
> We've all seen something on the Internet we disagree with or have received unwanted communication. Such behavior does not necessarily constitute online abuse. If you see or receive an @reply you don't like, unfollow and end any communication with that user.
>
> If the behavior continues, it is recommend that you block the user. Blocking will prevent that person from following you or seeing your profile picture on their profile page or in their timeline; additionally, their @replies or mentions will not show in your mentions tab (although these Tweets may still appear in search).
>
> Abusive users often lose interest once they realize that you will not respond. If the user in question is a friend, try addressing the issue offline. If you have had a misunderstanding, it may be possible to clear the matter up face to face or with the help of a trusted individual.
>
> If you continue receiving unwanted, targeted and continuous @replies on Twitter, and feel it constitutes online abuse, consider reporting the behavior to Twitter here.
>
> **Take threats seriously**
>
> If you believe you are in physical danger, contact the local law enforcement authorities who have the tools to address the issue.

> If you decide to work with law enforcement, make sure to do the following:
>
> document the violent or abusive messages with print-outs or screenshots
>
> be as specific as possible about why you are concerned
>
> provide any context you have around who you believe might be involved, such as evidence of abusive behavior found on other websites
>
> provide any information regarding previous threats you may have received

Instagram's community guidelines state that it will remove content that "contains credible threats or hate speech, content that targets private individuals to degrade or shame them, personal information meant to blackmail or harass someone, and repeated unwanted messages." There is a section for reporting bullying and harassment.

Snapchat's community guidelines have strictures about, amongst other things, threats and violence and harassment and bullying. There is a safety centre giving links to relevant organisations, research and news and where concerns can be reported.

8.2 The challenge for social media companies

The Home Affairs Committee said media and tech companies should do more to combat online hate, abuse and extremism.

In their 2017 Hate Crime report, the Home Affairs Committee criticised social media companies for not doing enough:

> We recognise that many social media and technology companies—including Google, Facebook and YouTube who gave evidence to our inquiry—have considered the impact that online hate, abuse and extremism can have on individuals. We welcome the effort that has been made to reduce such behaviours on social media, such as publishing clear community guidelines, building new technologies and promoting online safety, for example for schools and young people. However, it is very clear to us from the evidence we have received that nowhere near enough is being done. The biggest and richest social media companies are shamefully far from taking sufficient action to tackle illegal and dangerous content, to implement proper community standards or to keep their users safe. Given their immense size, resources and global reach, it is completely irresponsible of them to fail to abide by the law, and to keep their users and others safe. [56]

The Committee called the companies' reliance on users to report content "in effect, outsourcing the vast bulk of their safeguarding responsibilities at zero expense".[57] The report recommended that "all social media companies introduce clear and well-funded arrangements for proactively identifying and removing illegal content."[58] It suggested that the police ought to be able to recover the costs of enforcement from those companies.[59] The report also criticised a lack of transparency:

---

56 Home Affairs Committee, Hate crime: abuse, hate and extremism online, 1 May 2017, HC 609 2016-17, para 25
57 Ibid, para 31
58 Ibid, para 32
59 Ibid, para 33

> It is unacceptable that Twitter, Facebook and YouTube refused to reveal the number of people that they employ to safeguard users or the amount that they spend on public safety initiatives because of "commercial sensitivity". These companies are making substantial profits at the same time as hosting illegal and often dangerous material; and then relying on taxpayers to pay for the consequences. These companies wield enormous power and influence and that means that such matters are in the public interest.[60]

Facebook has appointed more moderators.

In May 2017, the Guardian reported that Facebook had announced that it would appoint 3,000 additional content moderators (on top of the 4,500 which the paper says it already has[61]) to remove content more quickly in the wake of broadcastings of killings and assaults.[62] Later in the same month, the Guardian ran a series of articles based on analysis of Facebook's moderation documents which, the paper said, showed the scale of the challenge which moderators face:

> The site has been accused of becoming a playground for misogynists and racists – a forum for fake news, threats, crudity and bad taste.
>
> Its users, who number nearly 2 billion, and its critics are asking: how did it come to this?
>
> And how is Facebook trying to balance valid concerns about reducing harm with the public interest in a free flow of information?
>
> Some of the answers lie in Facebook's "moderation" documents, which can be revealed by the Guardian. They detail what can and cannot exist on the site – and the scale of the challenge faced by moderators, who have spoken out about how difficult and confusing their job has become.[63]

Facebook's head of global policy management responded in an article saying that the Guardian's reporting got "a lot of things right":

However, the scale of the task is vast.

> On an average day, more than a billion people will use Facebook. They will share posts in dozens of languages: everything from photos and status updates to live videos. A very small percentage of those will be reported to us and investigated by our moderation teams. The range of issues is broad – from bullying and hate speech to terrorism and war crimes – and complex. Designing policies that both keep people safe and enable them to share freely means understanding emerging social issues and the way they manifest themselves online, and being able to respond quickly to millions of reports a week from people all over the world.[64]

In an article on Inform's Blog, a senior law lecturer argued that it is unusual for social media platforms to take responsibility for checking

---

60 Ibid, para 45

61 "Facebook moderators: a quick guide to their job and its challenges", Guardian, 21 May 2017

62 "Facebook Live: Zuckerberg adds 3,000 moderators in wake of murders", Guardian, 3 May 2017

63 "Has Facebook become a forum for misogyny and racism?", Guardian, 21 May 2017

64 "At Facebook we get things wrong – but we take our safety role seriously", Monica Bickert, Guardian, 22 May 2017

stories or identifying authors of cyberbullying, hate speech or other undesirable or criminal activity for two main reasons:

> Firstly, due to the volume of users, monitoring content is extremely difficult for social media platforms (indeed, in relation to Internet Service Providers monitoring such content is arguably impossible). An issue that animates this that has been the subject of widespread news coverage relating to online bullying is anonymous and pseudonymous expression, and the tensions this has created between free speech principles and the real name policies of social media platforms. Facebook's anonymity and pseudonymity policy relies on users to report fellow users using pseudonyms. However, in many instances, it is likely that these users will have no idea that a pseudonym is being used. Notwithstanding this, from a practical perspective, it is almost impossible for platforms such as Facebook to monitor and vet the millions of messages carried each week.
>
> (…)
>
> Secondly, there has been a disinclination amongst social media companies to play the role of arbiter, as this leaves them open to claims of censorship. This particular challenge, and the tension it creates, is illustrated by Facebook's reaction to the criticism referred to above in relation to the US election and fake news. The platform announced that it will work with a third-party fact-checking organisation whilst, at the same time, and rather contradictorily, reiterating its commitment to 'giving people a voice' and that it 'cannot become an arbiter of truth', with Mark Zuckerberg stating:
>
> 'We believe in giving people a voice, which means erring on the side of letting people share what they want whenever possible. We need to be careful not to discourage sharing of opinions or to mistakenly restrict accurate content.' [65]

There are issues not only with the volume of users, but also with anonymity and potential accusations of censorship.

Further insight into how Google, Facebook and Twitter deal with undesirable material was provided in an evidence session which formed part of the Home Affairs Committee's inquiry into hate crime. Twitter's Senior Public Policy Manager for the UK and Israel, Nick Pickles, responded to a question about how long it normally takes the company to deal with reported complaints:

> We want to get to every report as quickly as possible. One of the challenges about Twitter is that we see real-world events breaking on it. In the case of terrorist attacks, we will divert resources to deal with the reports coming in related to it, and that might mean that in other areas we are slower as a result. We take our resource and we prioritise accordingly. We prioritise reports of violent threats, for example. On your question about technology, one of the things we are trying to explore is how to use technology to better prioritise, so that we can be quicker. We have already made some changes internally on how we figure out whether two people have reported the same content, which several years ago we were not doing. We want to be faster, and we want to get to them

65 "Facebook's Frankenstein's Monster: freedom of expression and the problem with fake news and violent and sexual content – Peter Coe", Inform's Blog, 24 May 2017

> quicker. We are using technology as well as people's reports to do that.[66]

He highlighted recent changes Twitter was making:

> One of the things we are currently working on is how to use technology, as well as people, to identify those accounts for human review. For those kinds of violent threat that break our rules, we want to find a balance: as well as user reports, we want to proactively find those accounts for review, even if they are not reported. We have started rolling that technology out in recent weeks. That is a step change in how we deal with abuse—we are looking for it, and we will take action on content, even where it has not been reported by users.[67]

Nick Pickles went on to make it clear that pre-moderation was not possible:

> Let us be absolutely clear: we are never going to get to a point where internet companies pre-moderate content for the 400 hours of YouTube going up every day and for the 500 million tweets that go up every day. If you want pre-moderation of internet platforms, there may well be no internet platforms. I think we need to be very, very clear about how we discuss this, because there is a scale challenge. The positive benefits that our platforms bring and technology brings—yes, it comes with serious challenges. Yes, it brings out some of the worst in society and it brings to light things that we would all rather did not happen. But the idea that you can pre-emptively detect things and then remove them before they have been posted—we are never going to get to that point, and I think we need to be honest about that.[68]

---

66 Home Affairs Committee, Hate crime and its violent consequences – oral evidence, HC 609, 14 March 2017, Q440
67 Ibid, Q441
68 Ibid, Q471

9. Sources of help and advice

Adults

Stop Online Abuse is an online resource which was launched in 2015 by Galop (the LGTB and anti-violence charity in consultation with Trans Media Watch, the Women's Resource Centre, Gender Identity Research and Education Society, Rights of Women, Allsorts and the LGBT Consortium.[69] It states:

> Whilst online abuse can affect anyone, women and LGBT people often experience abuse as a result of their sex, gender identity or sexual orientation - or may be targeted for these reasons. The aim of this website is to provide support and guidance to people who are experiencing this type of online abuse.

The website has a range of resources including information on using the law.

The Revenge Porn Helpline, funded by the Government Equalities Office, is a dedicated service supporting victims of image based abuse.[70] They offer assistance in reporting and removing content, as well as advice and support on how to gather evidence. The helpline is available on 0845 6000 459.

Further cyber security advice can be found on the Government's website Cyber Streetwise and on the Government supported website Get Safe Online.

Parents and children

There are various websites and organisations giving advice and information for parents and children. These include:

- NSPCC website - Bullying and cyberbullying
- Childline website - cyberbullying
- Bullying UK website - cyberbullying
- Parentzone
- Childnet
- Internet matters
- UK Safer Internet Centre

The UK Council for Child Internet Safety (UKCCIS) brings together government, industry, law enforcement, academia, charities and parenting groups to help to keep young people safe online. UKCCIS has published a guide for parents and carers whose children are using social media.

The Child Exploitation and Online Protection Centre (CEOP) is part of the National Crime Agency and provides a ThinkUKnow website which gives a range of advice to parents, teachers (and children).

---

69 It carries the logos of these organisations and that of the Government Equalities Office.

70 The service has been funded by Government since its launch. See Government Equalities Office, Revenge porn helpline given further funding, 8 April 2017.

10. Scotland

10.1 The law

As in England and Wales, there are a number of offences which can cover online bullying and harassment. These include:

- The common law offences of breach of the peace and threats
- threatening and abusive behaviour - section 38 of the Criminal Justice and Licensing (Scotland) Act 2010
- stalking - section 39 of the Criminal Justice and Licensing (Scotland) Act 2010 (which preceded the stalking offences introduced in England and Wales)[71]
- improper use of a public electronic communications networks - section 127 of the Communications Act 2003 as amended[72]

Sections 8-10 of the Protection from Harassment Act 1997 cover Scotland and provides civil remedies for those suffering from harassment. See Library Briefing Paper 6648 for further details.

As in England and Wales, the Scottish Parliament has introduced an offence to deal with this issue. Section 2 of the Abusive Behaviour and Sexual Harm (Scotland) Act 2016 creates a new offence of disclosing, or threatening to disclose, an intimate photograph or film.[73] Section 2 is not yet in force.

10.2 Guidance and help for victims

In December 2014, the COPFS published guidance on communications sent via social media "to provide clarity on when such communications will amount to criminal conduct".[74]

The Scottish Government provides a full list of legislation relevant to all aspects of online safety, including the safe and responsible use of mobile technology

Citizens Advice Scotland provides practical information on taking action about harassment in Scotland.

The NSPCC provides information pages on Online Abuse: Legislation, policy and practice, in all four countries of the UK, including Scotland.

Respect*me* is Scotland's national Anti-Bullying Service. Its guide includes a section on online bullying.

---

71 See Library Briefing Paper 6261, Stalking: Criminal Offences
72 Scottish Parliament SP WA S4W-06345, 10 April 2012
73 Further background to the 2016 Act is available from the Abusive Behaviour and Sexual Harm (Scotland) Bill of the Scottish Parliament website
74 "Crown Office sets out social media prosecution policy", COPFS news release, 4 December 2014

11. Northern Ireland

11.1 The law

As in England and Wales and Scotland, there are a number of offences which can cover online bullying and harassment. These include:

- improper use of a public electronic communications network - section 127 of the Communications Act 2003 as amended
- harassment – The Protection from Harassment (Northern Ireland) Order 1997 (SI 1997/1180/N.I. 9) as amended
- Sending a "letter or other article" (including an electronic communication) to someone with the intention of causing anxiety or distress to that person - article 3 of the Malicious Communications (Northern Ireland) Order 1988 (SI 1988/2849 /N.I. 18)

11.2 Guidance and help for victims

The Department for Education Northern Ireland has a web page, Internet and wifi guidance which lists a range of guidance on acceptable and safe use of the internet and includes Circular 2016/27 on online safety which covers online bullying.

The Police Service Northern Ireland provides information on Harassment and Stalking, including a leaflet, Stalking and harassment: advice and information.

The Northern Ireland Anti-Bullying Forum has a guide to Cyber bullying and the Law in Northern Ireland

Victim Support Northern Ireland provides information and support to victims, and has a page on ECrime which covers what to do about cyber bulling, trolling and other kinds of online harassment.

BRIEFING PAPER
Number 07967
9 June 2017

About the Library

The House of Commons Library research service provides MPs and their staff with the impartial briefing and evidence base they need to do their work in scrutinising Government, proposing legislation, and supporting constituents.

As well as providing MPs with a confidential service we publish open briefing papers, which are available on the Parliament website.

Every effort is made to ensure that the information contained in these publicly available research briefings is correct at the time of publication. Readers should be aware however that briefings are not necessarily updated or otherwise amended to reflect subsequent changes.

If you have any comments on our briefings please email papers@parliament.uk. Authors are available to discuss the content of this briefing only with Members and their staff.

If you have any general questions about the work of the House of Commons you can email hcenquiries@parliament.uk.

Disclaimer