House of Commons

Petitions Committee

# Tackling Online Abuse

## Second Report of Session 2021–22

*Report, together with formal minutes relating to the report*

*Ordered by the House of Commons*
*to be printed 25 January 2022*

**HC 766**
Published on 1 February 2022
by authority of the House of Commons

## Petitions Committee

The Petitions Committee is appointed by the House of Commons to consider e-petitions submitted on petition.parliament.uk and public (paper) petitions presented to the House of Commons.

### Current membership

Catherine McKinnell MP (*Labour, Newcastle upon Tyne North*) (Chair)

Tonia Antoniazzi MP *(Labour, Gower)*

Elliot Colburn MP *(Conservative, Carshalton and Wallington)*

Martyn Day MP (*Scottish National Party, Linlithgow and East Falkirk*)

Katherine Fletcher MP *(Conservative, South Ribble)*

Nick Fletcher MP *(Conservative, Don Valley)*

Jonathan Gullis MP *(Conservative, Stoke on Trent North)*

Tom Hunt MP *(Conservative, Ipswich)*

Taiwo Owatemi MP *(Labour, Coventry North West)*

Christina Rees MP *(Labour, Neath)*

Matt Vickers MP *(Conservative, Stockton South)*

### Powers

The powers of the Committee are set out in House of Commons Standing Orders, principally in SO No. 145A. These are available on the internet via www.parliament.uk.

### Publications



Committee reports are published on the Committee's website and in print by Order of the House.

### Committee staff

The current staff of the Committee are Sabbir Ahmad (Committee Operations Officer), Zoe Backhouse (Head of Petitions Engagement), Gary Connor (Media Relations Manager), Ed Faulkner (Second Clerk), Stella-Maria Gabriel (Committee Operations Manager), Hannah Olbison (Senior Media Relations Officer), Shane Pathmanathan (Petitions Moderation and Data Manager), Duncan Sim (Committee Specialist), Ben Sneddon (Clerk), and Stephen Wilson (Senior Petitions Communications and Engagement Manager).

All correspondence should be addressed to the Clerk of the Petitions Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 4887; the Committee's email address is petitionscommittee@parliament.uk.

You can follow the Committee on Twitter using @HoCpetitions

# Contents

# Summary

The fantastic opportunities offered by the online world, and social media in particular, to communicate and connect with other people are too often misused by some to threaten, abuse, or demean others. These actions can significantly affect the health and wellbeing of people who receive abuse and their families, and erode their ability to speak freely online. While any user of social media and other online platforms may be the victim of this behaviour, online abuse poses a particular risk of harm to some groups—including children, as well as people from communities who face higher levels of abuse online such as disabled people, LGBT+ people, people from minority ethnic backgrounds, and women.

The popularity of e-petitions we have received in recent years on this issue demonstrates how strongly people believe that something needs to be done. One petition, the most popular created on our website in 2021, was signed by over 500,000 people in the weeks following the racist abuse aimed at black England footballers on social media last summer.

A report by the Petitions Committee in the 2017–19 Parliament highlighted the failure of social media companies to tackle online abuse through self-regulation. Since then, many companies have developed new technologies and tools to help keep users safe on their platforms. Yet progress in detoxifying online spaces has been limited, and will remain so for as long as these companies can choose to prioritise user engagement over user safety. We therefore welcome the Government's intent to impose legal requirements on these companies to address harmful content on their platforms, through the forthcoming Online Safety Bill.

The Government published a draft version of the Bill in May 2021. We welcome the strong duties the Bill would place on platforms to address criminally abusive content and behaviour, and to protect children from encountering harmful material. However, we call for the Bill to be strengthened, especially in its approach to abuse that is not illegal but is still harmful:

- The Bill should set a clear standard of protection adult users can expect against abuse on social media platforms, rather than leaving individual platforms to decide this in their rules on acceptable content. It should also encourage companies to make changes to how their platforms work to reduce the risk of abuse occurring or being seen by large numbers of adult users in the first place. To achieve these outcomes, we recommend that the Government imposes a foundational general duty on platforms to protect their users from reasonably foreseeable risks of harm.

- The Government should consider whether the Bill's duties to protect children and adults from legal but harmful content (including abuse) should apply to smaller as well as larger platforms. This could help to ensure that this content is not simply displaced onto smaller platforms where it may continue to fuel prejudice and cause real-world harm, including to children.

- The Bill should respond to the disproportionate abuse faced by some groups of people online. It should require social media companies to specifically consider the heightened risks faced by users from these groups when deciding how to protect their users' safety. It should also explicitly require platforms to take action to address abuse aimed at one or more people on the basis of characteristics (such as race, sexuality, gender or disability) which are already protected under the Equality Act and hate crime laws, as well as violence against women and girls.

However, tackling online abuse is more than a matter of changing what people can post or see on social media. Addressing this problem also means challenging the attitudes that fuel such abuse, and educating both young people and adults about acceptable and supportive online behaviour. The petitions that prompted our inquiry argued that more should be done to hold people accountable for their actions online, both to prevent abusive users from returning to social media platforms and to ensure that they face legal sanctions for their behaviour where appropriate.

It is welcome that the Government is considering changes to the law relating to online communications following the Law Commission's recent review, and also potentially on hate crime—including changes to the definition of disability hate crime called for in the Petitions Committee's report in the last Parliament. The Government should keep the impact of any new criminal offences relating to online communications under review, including their effects on freedom of speech. We also recommend that the Government re-examines whether the police and prosecutors have the resources and training they need to effectively enforce the law in this area.

We considered the proposal made in a popular e-petition last year to require users of social media platforms to link their account to verified ID. We support the idea that users should be able to verify their identity on a voluntary basis and block interactions with unverified users, allowing people to add an extra layer of protection to their online experience if they want it. We also recommend that the Government requires social media companies to specifically assess and address the risks which come from allowing people to use anonymous accounts. Social media companies should face fines if they cannot demonstrate that they are successfully preventing people who they have banned for abusive behaviour from setting up new accounts.

We are grateful to everyone who started or signed petitions, gave evidence to us, or took part in our sessions with schools. In considering this report and other recent work in Parliament on this issue, we urge the Government to listen to the hundreds of thousands of petitioners who have pushed for change, and to make this the watershed moment when the menace of online abuse is finally tackled.

**Box 1: About this report**

This report is a House of Commons Select Committee report. A Select Committee is a cross-party group of MPs that can publish reports calling on the Government to take action on an issue. We are the Petitions Committee: we schedule debates on e-petitions and run inquiries which investigate problems that people raise through e-petitions.

This report investigates the problem of online abuse. This is an issue that has been raised in multiple e-petitions that have gained hundreds of thousands of signatures in recent years. Like most Select Committee reports, it has been informed by views we have heard from people and organisations who have either told us their views in writing through written evidence or spoken directly to us in oral evidence. For this inquiry, we also heard the views of secondary school students across the UK in specially organised school sessions. Many young people have grown up using social media, and we wanted to hear students' ideas and insights on how the problem of online abuse might be addressed. We have used this evidence to draw conclusions and make recommendations for the Government and other bodies to act on.

Our report follows on from a report by the previous Petitions Committee in the last Parliament, *Online abuse and the experience of disabled people,* which highlighted the scale of the problem and the harm it can cause. Since that report, which was published in 2019, the Government has set out its plans for new legal requirements on social media platforms to tackle online abuse. It did this through the draft Online Safety Bill (you can find more information in Box 2 about the Bill). Our new report examines the detail of the Government's proposals, to see if they will help to resolve the problem of online abuse. We make suggestions about how we think the Government can improve its plans. The Government has to consider and respond to our suggestions, and our recommendations might go on to inform how MPs debate the proposed new law in Parliament. The Government doesn't have to accept our recommendations.

One of the most popular petitions of 2021, started by Katie Price, called on the Government to require social media users to provide ID before they can set up an account. Because so many people supported this petition, we've specifically looked at the advantages and disadvantages of this idea, including asking the school students who we spoke to for their views. We also asked the students what they thought about other possible technological or education-based responses to the problem of online abuse. We hope their views will inform specific actions that the Government and Ofcom (the new online safety regulator) might take to address the problem of online abuse in future.

# 1 Introduction

## Background

1. Social media offers fantastic opportunities to interact with others, but can also facilitate the sending of hateful and demeaning communications, harassment, and other forms of threatening and violent behaviour. In addition to the serious harm such content can cause to the individuals who are its direct targets, online abuse also has a corrosive effect on online spaces, reducing people's willingness to express themselves and engage with others.[1] The online world's potential for both benefit and harm was expressed to us by Bobby Norris, creator of the petition that prompted this inquiry:

> I'm not here to bash social media. I love it, and 95% of it is an amazing tool […] When used in the right way, it's amazing, and especially during lockdown I'm so glad that we have technology so that […] we have been able to connect with friends and family while self-isolating. But there is a very dark side to social media as well.[2]

The scale of public concern about abusive online behaviour is shown by the popularity of e-petitions we have received on this subject in recent years.[3]

2. In January 2019 the Petitions Committee published its report on online abuse of disabled people. This found that disabled people faced an "extreme level of abuse" online, and highlighted how this can destroy their social lives and do lasting damage to their health.[4] It concluded that social media companies had failed to conduct "responsible self-regulation" in allowing toxic online environments to take hold, and that the Government should take steps to address this failure.[5] It also drew attention to the lack of legal sanctions for often appalling content, and concluded that the law on online abuse was "not fit for purpose".[6] The Government's response to the report in April 2019 acknowledged "the disproportionate abuse experienced by disabled people online and the damage such abuse can have on people's lives, career and health", and stated a forthcoming Online Harms White Paper (published in April 2019)[7] would set out measures to help keep all UK internet users safe.[8]

3. Following consultation on the Online Harms White Paper,[9] the Government published a draft version of its Online Safety Bill in May 2021.[10] This Bill would establish

1 See paragraphs 16–17 on how online abuse impacts people who are targeted by this behaviour; and paragraph 36 on how abuse can restrict some groups' freedom of expression online
2 Q2
3 See paragraphs 5–8 and Boxes 3 and 4 below for details of popular e-petitions on online abuse since 2019
4 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, Summary (page 3) and para 54
5 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 83–86
6 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 91–97 and 101–103
7 Department for Digital, Culture, Media and Sport and Home Office, Online Harms White Paper, CP 57, 8 April 2019
8 Petitions Committee, Second Special Report of Session 2017–19, Online abuse and the experience of disabled people: Government response to the Committee's First Report, HC 2122, Introduction (page 1)
9 Department for Digital, Culture, Media and Sport and Home Office, Consultation outcome: Online Harms White Paper, 15 December 2020 [last updated] (accessed 18 January 2022)
10 Department for Digital, Culture, Media and Sport, Draft Online Safety Bill, CP 405, 12 May 2021

a new statutory regulatory framework for social media and other online platforms; more information about the Bill is set out in Box 2 below. A Joint Committee of the House of Commons and the House of Lords set up to conduct pre-legislative scrutiny of the draft Bill reported in December 2021,[11] and the Government has said the Bill will be introduced to Parliament before the end of this Parliamentary session.[12]

**Box 2: The Online Safety Bill**

The Online Safety Bill is a proposed new law, which the Government plans to introduce in the coming months. It will impose new legal requirements on social media and other online platforms. This includes any platform which enables UK users to post content such as comments, images or videos, or to talk to others online via messaging or forums.

The Bill will require platforms to take steps to protect the safety of people who use their services. Under the Bill, platforms will have to:

- Identify whether they are hosting any content which is illegal or risks harming people, and if so, take action to respond to it;
- Protect users' freedom of expression;
- Offer effective ways for users to report harmful content, and to complain if they feel a platform is failing to protect their safety or has unfairly removed content they have posted; and
- Publish transparency reports, which may include information such as how much harmful content there is on the platform and how the platform is responding to this.

The Bill will also give Ofcom the power to act as a new online safety regulator. Ofcom will have the power to fine platforms that don't meet their new responsibilities. We examine the Bill in further detail in Chapter 4.

Source: Department for Digital, Culture, Media and Sport, Draft Online Safety Bill

4. We are one of several Parliamentary committees to have examined the issue of online harms. In addition to the work of the Joint Committee on the Draft Online Safety Bill, the Digital, Culture, Media and Sport Committee has considered topics including what lessons can be learned from other countries' approaches to online safety,[13] and has recommended that the Government take action against legal online content that contributes to online violence against women and girls and child sexual exploitation;[14] the Home Affairs Committee has looked at how social media can facilitate illegal activity such as human trafficking, as well as holding a session specifically examining online racist abuse of footballers after the European Championships final;[15] and the House of Lords Communications and Digital Select Committee has reported on online freedom of expression.[16]

11 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609

12 The Secretary of State for Digital, Culture, Media and Sport, Rt Hon Nadine Dorries MP, told the Digital, Culture, Media and Sport Committee in November 2021 that the Government intends to introduce the Bill to Parliament in March 2022 or sooner. See oral evidence taken before the Digital, Culture, Media and Sport Committee on 23 November 2021, HC 44, Qq248–251

13 Digital, Culture, Media and Sport Sub-Committee on Online Harms and Disinformation, Online safety and online harms, HC 620

14 Digital, Culture, Media and Sport Committee, Eighth Report of Session 2021–22, The Draft Online Safety Bill and the legal but harmful debate, HC 1039

15 Home Affairs Committee, Online Harms, HC 624

16 Communications and Digital Committee, First Report of Session 2021–22, Free for all? Freedom of expression in the digital age, HL Paper 54

## Petitioners' campaigns and our inquiry

5. In February 2019, Bobby Norris created an e-petition calling for online homophobia to be made a specific criminal offence.[17] It highlighted the prevalence of homophobic abuse online and the impact that receiving abusive messages had had on his personal mental health, and suggested a specific criminal offence was needed to punish users sending these messages. The petition received over 153,000 signatures and was debated in Westminster Hall in July 2019.[18] The Government response, provided in March 2019, pointed to then-ongoing reviews by the Law Commission into hate crime and online communications offences, and said the Government would consider reforms when these reviews were published.[19] We discuss the outcomes of these (now published) reviews in Chapter 5.

6. Bobby Norris started a second petition in September 2019, which called on the Government to ensure online "trolls" can be held accountable for their actions via their IP address.[20] It attracted over 133,000 signatures before it closed early due to the 2019 General Election; the full text of the petition is set out in Box 3 below. The Government's response to the petition, provided in September 2019,[21] stated that it would establish a legal duty of care for social media companies to protect their users from harm. However, it also argued it would not be appropriate to require a specific technological response to online abuse which might become outdated or defunct. The Government has now published its proposed online safety legislation in draft, which we examine in Chapter 4. We discuss the specific issue of ensuring previously banned users are prevented from returning to social media platforms in Chapter 6.

**Box 3: Bobby Norris' second 2019 petition**

**Hold online trolls accountable for their online abuse via their IP address**

It's far too easy for online trolls to just create another email address and another social media account if they have their accounts suspended.

However, if their internet service providers were required to block their access to social media, and social media companies blocked their IP addresses, it would be far harder for them to get another account and continue their abuse.

Source: e-petition 272087

7. We opened this inquiry in early 2020, to follow up on the commitments made by the Government in its response to our predecessor Committee's report, and in light of the popularity of Bobby Norris' second petition. In spring 2020, we took oral evidence from Bobby Norris[22] and from Katie Price,[23] who created the petition which prompted our predecessor Committee's inquiry during the 2017–19 Parliament,[24] together with her mother Amy. The inquiry was then paused during the early stages of the covid-19 pandemic to enable the Committee to focus on issues raised in e-petitions relating to

17 e-petition 239444, Make online homophobia a specific criminal offence
18 HC Deb, 1 July 2019, cols 419–444WH
19 Home Office, response to e-petition 239444, 28 March 2019
20 e-petition 272087, Hold online trolls accountable for their online abuse via their IP address
21 Department for Digital, Culture, Media and Sport, response to e-petition 272087, 24 September 2019
22 Qq1–13
23 Qq14–60
24 e-petition 190627, Make online abuse a specific criminal offence and create a register of offenders. The petition attracted over 220,000 signatures before it closed early due to the 2017 General Election

the Government's response to the pandemic. We resumed our inquiry following the publication of the Government's draft Online Safety Bill in May 2021, as well as the success of a new petition created by Katie Price in March 2021 calling on the Government to make verified ID a requirement for opening a social media account.[25] The full text of the petition is set out in Box 4 below.

**Box 4: Katie Price's 2021 petition**

**Make verified ID a requirement for opening a social media account**

Make it a legal requirement when opening a new social media account, to provide a verified form of ID. Where the account belongs to a person under the age of 18 verify the account with the ID of a parent/guardian, to prevent anonymised harmful activity, providing traceability if an offence occurs.

My son Harvey is disabled. He is also the kind and gentle son of a person regularly in the public eye. The Online Harms Bill doesn't go far enough in making online abuse a specific criminal offence and doing what 'Harvey's Law' intended. To make the law work needs the removal of anonymity to ensure that users cannot cause harm by using online platforms to abuse others. Where an offence has taken place they ought to be easily identified and reported to the police and punished. We have experienced the worst kind of abuse towards my disabled son and want to make sure that no one can hide behind their crime.

Source: e-petition 575833

8. Katie Price's petition received almost 700,000 signatures before it closed in September 2021, over 500,000 of which came in the weeks following the racist abuse aimed at black England footballers on social media after the 2020 European Championships final. The Government's response to the petition, provided in May 2021,[26] acknowledged that anonymity online can be linked to bad actors and harmful activity. However, it also noted a range of social media users rely on online anonymity for their personal safety, which compulsory user ID verification could put at risk. It stated the police already have a range of legal powers to identify individuals who engage in illegal online activity anonymously, and argued the Online Safety Bill would address both illegal and "legal but harmful" abuse whether or not it was posted anonymously. We examine the issue of user traceability by law enforcement, as well as the question of identity verification on social media, in Chapter 6.

9. To inform our report, we took evidence from a range of stakeholders, including hearing from Bobby Norris and Katie and Amy Price about their personal experiences of online abuse being targeted at them and their families. We also heard from civil society organisations representing users most vulnerable to or most likely to face abuse online; legal experts; groups with an interest in freedom of speech online; experts in regulatory and technological responses to online harms; and representatives from three major social media companies. We concluded our inquiry by hearing from the relevant Minister and an official from the Department for Digital, Culture, Media and Sport.

10. As part of our inquiry, we also engaged with students aged between 13 and 18 to get their views on how social media companies and the Government should respond to online abuse. The minimum age for many social media platforms is 13, and young people

25 e-petition 575833, Make verified ID a requirement for opening a social media account

26 Department for Digital, Culture, Media and Sport, response to e-petition 575833, 5 May 2021

are a major part of many platforms' user bases. We designed a session that was run in 12 schools in October and November 2021, and the responses of over 500 young people were fed back to us; Members of the Committee also attended four of the sessions. A summary of the views we heard from students during the engagement sessions, and in the responses they provided to us, is included as an Annex to this report.[27]

11. We are hugely grateful to all of those who contributed to our work—our expert witnesses for their knowledge and insight; the students who participated in our public engagement sessions for their ideas and enthusiasm, as well as Parliament's Education and Engagement and Select Committee Engagement teams, in particular Sky Yarlett, for their support in organising and delivering the sessions; and Bobby Norris and Katie Price for starting their petitions and courageously sharing their personal experiences with us, and everyone who signed the petitions that have prompted and informed this report.

27 See Annex: Summary of school engagement

# 2 The experience of people receiving online abuse

## The scale of online abuse

12. While the petitions that prompted our inquiry were started by high-profile individuals with personal experience of abuse being sent to them and their families online, the experience of receiving online abuse is not confined to people with public profiles and large numbers of followers. Research by the Alan Turing Institute has previously estimated that 10–20% of people in the UK have been personally targeted by abusive content online.[28] Ofcom's pilot Online Harms Survey for 2020/21 found that in a four-week period, 13% of survey respondents had experienced trolling, 10% offensive or upsetting language, and 9% hate speech or speech encouraging violence.[29] Petitioner Bobby Norris, while highlighting his own experience of receiving abuse, told us: "speaking about it to my fans and followers on social media, I am so aware that it's not just me and people in the public eye going through it".[30]

13. Witnesses representing organisations that campaign on behalf of specific groups of users of online platforms described the scale of online abuse targeted at or otherwise encountered by those groups. Danny Stone from the Antisemitism Policy Trust told us that antisemitism online is "widespread and pervasive", and that an increasing proportion of antisemitic behaviour was occurring online.[31] Nancy Kelley from Stonewall referred to research by the charity Galop in 2020, which found that 78% of LGBT+ people had experienced anti-LGBT+ abuse or hate speech online in the previous five years; of those who reported receiving abuse, 97% reported having been insulted, 63% had been threatened with physical violence, and around 40% had faced threats of sexual assault and/or death threats.[32]

14. The evidence we took also echoed findings from research into online abuse in suggesting that abusive content was more commonly targeted at people with particular characteristics or from certain communities.[33] Nancy Kelley told us about 70% of lesbian, gay and bisexual adults have encountered online harassment, compared to about 40% of straight adults.[34] The Women's Aid Federation of England (Women's Aid) told us that "research consistently shows that women are subjected to more bullying, abuse, hateful language and threats online than men", and highlighted the increasing use of the online world to perpetrate Violence Against Women and Girls.[35] Seyi Akiwowo from Glitch cited evidence from Amnesty International showing that black women are 84% more likely to

28 The Alan Turing Institute, How much online abuse is there?, 27 November 2019 (accessed 18 January 2022)
29 Ofcom, Ofcom Pilot Online Harms Survey 2020/21, February 2021 (accessed 18 January 2022)
30 Q1
31 Q2 [Danny Stone]
32 Q2 [Nancy Kelley]. See Galop, Online Hate Crime Report 2020, 10 June 2020 (accessed 18 January 2022)
33 For example, the Alan Turing Institute has found experiences of online abuse vary by demographic factors including ethnicity and age, with younger people and people from Black ethnic backgrounds more likely to be targeted by abuse. See The Alan Turing Institute, How much online abuse is there?, 27 November 2019 (accessed 18 January 2022). As noted in paragraph 2, our predecessor Committee's 2019 report also pointed to the "extreme" levels of abuse faced by disabled people online.
34 Q2 [Nancy Kelley]
35 Women's Aid Federation of England (TOA0011)

be abused online than white women.[36] We also heard about the intersectional[37] nature of much online abuse: for example, Danny Stone highlighted the abuse faced by Jewish women online.[38]

15. We heard that the incidence of online abuse had increased since the start of the covid-19 pandemic. Petitioners Katie Price and Bobby Norris told us they had personally experienced increased abuse targeting them (and in Katie's case, her son Harvey) during the first lockdown in spring 2020.[39] Andy Burrows from the National Society for the Prevention of Cruelty to Children (NSPCC) told us the charity's Childline service had seen a 25% increase in counselling sessions relating to online bullying during the pandemic.[40] Seyi Akiwowo told us about Glitch's research into the online experiences of women and non-binary individuals during the early months of the pandemic: almost half of their survey respondents reported receiving online abuse during this period, almost a third of whom reported an increase in abuse over this time.[41] The charity Protection Approaches also cited increased incidents of online hate being targeted at people from the Chinese, Asian and Black communities they work with.[42]

## The impact of online abuse

16. Our predecessor Committee's 2019 report highlighted the effects of online abuse on the victims of this behaviour, including how it can specifically impact disabled people. These effects can include stress, depression and anxiety, which can in turn contribute to a worsening of any pre-existing or long-term health conditions. Abuse may also lead to people abandoning online profiles or having to change their contact details, contributing to social isolation and increased difficulty in taking on professional or other opportunities.[43] Other committees have also heard evidence from individuals who have received abuse online about the consequences this has had for their mental health.[44]

17. Witnesses to our inquiry spoke about the real-world impact online abuse can have on the wellbeing of recipients and their families. Bobby Norris told us he had heard of cases of people self-harming following abuse on social media,[45] while Katie Price highlighted

36 Q42 [Seyi Akiwowo]

37 Intersectionality in this context refers to the way in which the combination of multiple characteristics possessed by an individual which individually already make them more likely to face abuse online (for example, in relation to their gender, sexuality, or racial background) may have an additional effect on the volume or severity of abuse they receive.

38 Q2 [Danny Stone]

39 Q1 [Bobby Norris]; Q17 [Katie Price]

40 Q43 [Andy Burrows]

41 Q46 [Seyi Akiwowo]. This research sought to understand the experiences of women and non-binary individuals as a collective group; however, the researchers noted that the sample of non-binary respondents who participated in the research was "too small to draw any meaningful conclusions" about the specific experiences of non-binary individuals over this period. See Glitch and End Violence Against Women Coalition, The Ripple Effect: Covid-19 and the Epidemic of Online Abuse, 20 September 2020 (accessed 18 January 2022)

42 Protection Approaches (TOA0018)

43 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 51–53

44 See, for example, Oral evidence taken before the Home Affairs Committee on 8 September 2021, HC 624, Qq170, 192; and oral evidence taken before the Joint Committee on the Draft Online Safety Bill on 9 September 2021, HC 609, Q22

45 Q2

the impact of the abuse faced by Harvey on her other children.[46] Matthew Harrison from Mencap told us about the offline effects of the online abuse faced by people with learning disabilities:

> Experiencing online harms can lead to increased levels of isolation and seclusion in [a person's] own home. We know that that impacts life opportunities, whether that is employment or socialising. We also know that has an impact on a person's physical health as well.[47]

## Measuring abusive and hateful content online

18. Witnesses presented extensive evidence on the scale of online abuse and its harmful effects, but it was also suggested to us that future policymaking and debate would benefit from a better understanding of the prevalence of this content. Dr Bertie Vidgen from the Alan Turing Institute told us that there is a need to define and measure online abuse with more "precision", "consensus" and "standardisation".[48] In particular, we heard that online hate speech was often not reported by victims and was therefore not recorded or acted upon,[49] and that the Government should invest in "good, basic data" to understand the scale of online hate speech and the experiences of those targeted by it.[50] Dedicated online hate crime statistics have not been included in the Home Office's *Hate Crime in England and Wales* statistical bulletin since 2017/18 due to data quality concerns.[51]

19. Social media companies provided us with figures on the scale of abuse and hate speech they have identified on their platforms. Rebecca Stimson from Meta (formerly Facebook)[52] told us that about 0.03% of content viewed on Facebook is hate speech, and 0.15% of content viewed on Instagram is bullying and harassment.[53] Katy Minshall from Twitter told us that impressions on tweets that violate Twitter's rules account for less than 0.1% of impressions globally.[54] However, Andy Burrows suggested these figures were of limited value as they are based on the experience of a "general user" and did not reflect the experiences of users who are more vulnerable to or disproportionately likely to face abuse.[55]

20. We asked the Minister for Technology and the Digital Economy, Chris Philp MP, together with Orla MacRae, Deputy Director for Online Harms Regulation at the Department for Digital, Culture, Media and Sport, about the latest data the Government had on the scale of online abuse. The Minister said the Government was aware the problem was "huge" and "widespread", but could not provide specific figures; Orla MacRae said the evidence base on online abuse was "still emerging" and not yet "comprehensive".[56]

46 Q16
47 Q2 [Matthew Harrison]
48 Q75 [Dr Vidgen]
49 For example, Nancy Kelley told us that "fewer than half" of online hate crimes against LGBT+ people are reported, while Matthew Harrison described the available data on levels of online disability hate crime as "very poor". See Q15 [Nancy Kelley]; and Q18 [Matthew Harrison]
50 Q17 [Nancy Kelley]
51 House of Commons Library, Hate Crime Statistics, 26 November 2021 [last updated] (accessed 18 January 2022)
52 In October 2021, Facebook changed its corporate name to Meta. Individual platforms owned and run by the company, including Facebook, WhatsApp, Messenger and Instagram, did not change names
53 Q95 [Rebecca Stimson]
54 Q95 [Katy Minshall]
55 Q57 [Andy Burrows]
56 Q139

They pointed to provisions in the planned Online Safety Bill—including the information-gathering powers that the Bill would give to Ofcom as the new online safety regulator, and the transparency requirements it would impose on social media companies—as crucial in improving this situation and accessing information held by those companies that is currently "hidden".[57]

21. **Online abuse can have a devastating impact on those who are exposed to it, and we are alarmed at evidence suggesting the problem has worsened since the covid-19 pandemic began. While tackling this issue is important in making the online environment safer for everyone, it must be recognised that online abuse is disproportionately targeted at certain groups. The Government is right to acknowledge the extent of this problem but should assess and track the scale of this behaviour more precisely and comprehensively.**

22. ***As part of its role as the new online safety regulator, we recommend that Ofcom should regularly report on the incidence of online abuse, illegal hate speech, and Violence Against Women and Girls content on the largest social media platforms. This should include disaggregating estimates of the likelihood of a user encountering or being the target of abusive content according to characteristics including race, disability, sexuality, and gender, as well as differentiating between child and adult users.***

57 Q139 [Orla MacRae]; Q140

# 3 Social media and user safety

## Technological responses to online abuse

23. While online abuse does not only occur on the largest social media platforms, their size and profile make them the predominant focus for discussion of this issue. Most major social media companies have rules prohibiting abusive content including bullying, harassment, threatening behaviour, and hate speech.[58] However, our predecessor Committee's report in 2019 found that despite these rules, illegal and abusive content on these platforms had created "toxic environments" for many users. It argued companies needed to take more responsibility for tackling this problem—including ensuring their systems for reporting abusive content are easy to find and understand, and more proactively searching for and removing abuse from their platforms.[59]

24. The companies we heard from during our inquiry argued that a key change from the time of the previous Committee's report was the amount of abusive content they were able to detect and remove proactively using technology, rather than relying on user reports.[60] Rebecca Stimson from Meta suggested this had helped drive recent improvements in their enforcement of their rules on abusive content,[61] while Katy Minshall from Twitter noted this change reduced the burden on victims of abuse to report this behaviour.[62] This represents significant progress in line with the ambition set out in our predecessor Committee's report.

25. Alongside improvements in the enforcement of their rules, the companies also noted recent innovations in how they design their services and safety tools they offer users, intended to help protect users from abusive or other harmful content. Theo Bertram from TikTok argued that focusing on this, rather than content moderation in isolation, was key.[63] Likewise, Rebecca Stimson suggested that "detecting, finding and removing harmful content online is extremely important […] but we are also doing a lot about preventing harm from happening in the first place".[64] Platform design and user functionality innovations highlighted by the companies included:

- "Kindness prompts" encouraging users to reconsider posts which are detected as being potentially offensive or against the platform's rules, that we heard can deter such posts in up to four out of 10 cases;[65]
- Instagram and TikTok making their services "private by default" for users under 16, restricting other users' ability to interact with those users;[66]

58 For example, Facebook's community standards cover behaviours including Violence and incitement, Bullying and harassment, and Hate speech; Twitter's rules include policies on Violent threats, Abusive behaviour, and Hateful conduct; while TikTok's community guidelines include policies on Violent extremism, Harassment and bullying, and Hateful behaviour (all links accessed 18 January 2022)

59 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, Summary (page 3)

60 For example, Theo Bertram stated that 94% of content removed by TikTok was now removed before being reported by a user. See Q95 [Theo Bertram]

61 Q95 [Rebecca Stimson]

62 Q95 [Katy Minshall]

63 Q95 [Theo Bertram]

64 Q118 [Rebecca Stimson]

65 Q95 [Katy Minshall]; Q95 [Theo Bertram]; Q118 [Rebecca Stimson]

66 Q95 [Theo Bertram]; Q98 [Rebecca Stimson]

- Twitter's introduction of controls for users on who can reply to posts they send, and its trial of a "safety mode" feature to automatically prevent interactions with accounts that appear to be behaving offensively;[67]

- Twitter's experimentation with algorithm design "to try to reduce the visibility of tweets that look like they could be abusive".[68]

26. As an additional technological response to abusive behaviour, Bobby Norris suggested users who repeatedly behave abusively on social media should be prevented from accessing the platform via a block on their IP address.[69] The idea of blocking previously banned users from returning to a platform via the same device was also raised in our school engagement sessions.[70] We heard from Rebecca Stimson that this is a sanction Meta can already apply.[71] Some students in our engagement sessions also proposed other technological responses to abuse they would like to see, such as platforms automatically filtering out (rather than removing) offensive content, either for all users or users under a certain age. Other ideas we heard from students, and a summary of their thoughts on some of the tools we heard platforms already have in place, are included as an Annex to this report.[72]

## Gaps in platforms' responses to abuse

27. The companies we heard from told us that user safety was a priority for them.[73] However, other witnesses argued that—given the continuing scale of online abuse—social media companies are still not taking the issue seriously enough. We heard the Government's proposed online safety legislation could help to change this. Matthew Harrison from Mencap suggested regulating social media would help to address the "lack of consequences" for companies for not tackling the harms enabled by their platforms; he argued that "self-regulation has been tried, and at the moment it is just not working".[74]

28. Civil society groups we heard from argued that social media companies had systematically failed to prioritise user safety. Nancy Kelley of Stonewall suggested there was "a fundamental imbalance in power and investment within the companies", with long-term underinvestment in technology that could improve user safety as opposed to driving high user engagement with content on the platform.[75] Andy Burrows of the NSPCC suggested that companies' response to abuse on their platforms had been characterised by:

> At best […] a lack of investment, a lack of resource and lack of consideration into user safety and protecting children and young people […] But, at worst, we have seen a business model that is designed to produce outrage.[76]

67 Q105; Q118 [Katy Minshall]
68 Q105 [Katy Minshall]
69 Q4; Q13. As noted in Chapter 1, Bobby also made this suggestion in an e-petition he created during the 2017–19 Parliament: e-petition 272087, Hold online trolls accountable for their online abuse via their IP address (see Box 3 above for the full text of this petition, and paragraph 6 for more details)
70 See Annex: Summary of school engagement
71 Q127
72 See Annex: Summary of school engagement
73 Q103 [Theo Bertram]; Q117 [Katy Minshall]
74 Q9 [Matthew Harrison]
75 Q9 [Nancy Kelley]
76 Q43 [Andy Burrows]

He cited the design of platforms' content recommendation algorithms as an example of this failure—suggesting that Frances Haugen's disclosures about Facebook's practices had revealed "business decisions being taken not to adjust the algorithms in the face of very real world harm".[77]

29. Despite social media companies' claims about the increasing amounts of abuse they are able to detect automatically, some witnesses told us platforms are still failing to effectively enforce their rules against abusive or threatening content. Katie Price described how her son Harvey is repeatedly "mocked in a serious and disgusting way", including facing racist abuse and abuse relating to his disability, but that platforms "keep that on there" despite many platforms having rules against degrading or negative content in relation to protected characteristics.[78] Danny Stone from the Antisemitism Policy Trust suggested a number of factors potentially contributing to this failure, including platforms failing to employ enough human moderators or offer them sufficient training, and the technological difficulty of identifying abusive content automatically.[79]

30. Witnesses also raised concerns that platforms' rules may not always prohibit abusive content. Nancy Kelley said that, in her experience of attempting to get posts taken down, "it is quite instructive what is not considered to be against community standards".[80] Similarly, written evidence provided to the Joint Committee on the Draft Online Safety Bill by football organisations argued many social media platforms' terms of service have been repeatedly seen to be "insufficient" to effectively respond to abuse.[81] Bobby Norris told us:

> I feel that social media platform providers need to do more on where their threshold is and on what they see as acceptable […] In so many cases—nine out of 10—platform providers will come back to say, basically, that it not breaking their rules and regulations. My question is, "What do you have to do to break a rule or regulation?"[82]

The issue of platforms failing to remove content that appears to violate their rules, or deeming such content acceptable following user complaints, has also been examined by other committees.[83]

31. We also heard about issues in users' experience of platforms' systems for reporting abuse. Katie Price told us platforms' responses to user complaints about abusive comments remained poor, suggesting: "you report them but you never hear back".[84] This issue was also raised by students in our school engagement sessions: many students said that they felt that reporting abuse rarely led to anything and that they didn't know what happened when they reported abuse.[85] The Epilepsy Society told us that Twitter's response to their

77 Q47. Seyi Akiwowo likewise pointed to the design of these algorithms as an example of companies prioritising user engagement over user safety, suggesting that Facebook was "benefiting from outrage" while its algorithms were "amplifying and exacerbating gender-based abuse"; see Q42

78 Q15; Q26

79 Q9 [Danny Stone]

80 Q4 [Nancy Kelley]

81 The Football Association, The Premier League, EFL, and Kick It Out, Written evidence to the Joint Committee on the Draft Online Safety Bill, HC 609, OSB0007

82 Q7

83 See for instance, Oral evidence taken before the Home Affairs Committee on 8 September 2021, HC 624, Qq207–226

84 Q30

85 See Annex: Summary of school engagement

reports of users sending flashing images to people with epilepsy "was not rapid enough", putting people with epilepsy at risk of harm.[86] We also heard from Mencap that platforms had made only limited progress on the need—highlighted in the previous Committee's 2019 report[87]—to make their systems for reporting abuse accessible to disabled users, in particular providing easy read information.[88]

32. **Our predecessor Petitions Committee's report concluded that self-regulation of social media had failed. Despite the user safety tools and innovations platforms have introduced since then, these companies have continued to place insufficient priority on user safety to protect users from abusive and hateful behaviour on their platforms, or ensure users are able to effectively raise their concerns when subjected to this behaviour. We support the Government's intention to end social media self-regulation and introduce a statutory regulatory framework.**

86 Epilepsy Society (TOA0020)

87 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 79–80

88 Royal Mencap Society (TOA0015)

# 4 The Online Safety Bill

## Online abuse and the Bill

33. The Government has said that its planned Online Safety Bill will force social media companies to do more to tackle abuse on their platforms. In response to a Parliamentary Question in May 2021, then-Minister of State Caroline Dinenage MP stated:

> The Online Safety Bill, which has now been published in draft, will require all companies to take swift and effective action against hate speech and online abuse.[89]

The Minister, Chris Philp MP, told us that the draft Bill contains measures designed to tackle both illegal abuse (such as illegal hate speech or other abusive communications meeting a criminal threshold) and abusive content that is legal but that is harmful either to children or to adults.[90] Stephen Kinsella from campaign group Clean Up The Internet described the Bill as "a once in a generation opportunity" to help tackle online abuse and other online harms—but also noted this meant it was vital to "get it right".[91]

**Table 1: Platforms' safety duties under the draft Online Safety Bill (non-exhaustive)**

| Type of content | Platforms in scope | General duty | Content duty |
|---|---|---|---|
| Illegal content | All platforms | "Take proportionate steps to mitigate and effectively manage the risks of harm" to relevant users arising from this content | "Swiftly take down" such content when the platform becomes aware of it |
| Content harmful to children | Platforms "likely to be accessed" by children | | "Protect" children in age groups where this content poses a risk of harm from "encountering" such content |
| Content harmful to adults | "Category 1" platforms | None | Set, and consistently enforce, terms of service that specify how such content is to be "dealt with" by the platform |

Source: Draft Online Safety Bill, Sections 9–11. N.B. the list of duties presented in this table is for illustrative purposes only and is not intended to be an exhaustive representation of the full suite of safety duties outlined in the draft Bill.

89 PQ 2283 [on Social Media: Harassment], 21 May 2021
90 Q131
91 Q44

**Box 5: How will the Online Safety Bill work?**

The draft Online Safety Bill deals with three types of content: illegal content, content harmful to children, and content harmful to adults. Content is considered harmful if it presents a "material risk" of having "a significant adverse physical or psychological impact" on a child or adult. The draft Bill would also allow the Secretary of State to use secondary legislation to designate certain content as "priority" content and to specify that platforms must tackle content of this type. For example, this might be racist hate speech or racist abuse.

The new rules about illegal content in the Bill would apply to all online platforms. The Bill would also require all platforms to assess whether their service has or may attract a "significant number" of child users (known as the "child user condition"); if so, the platform must also comply with the duties to protect children. The rules on content harmful to adults apply only to "category 1" services, such as the largest social media platforms, where users face the greatest risk due to the number of users the platform has and the features it offers users.

Platforms will have to carry out risk assessments to understand how likely it is that people will come into contact with illegal or harmful content on the platform. These risk assessments must also consider how much the platform's own content recommendation algorithms, and other features they offer users, contribute to the posting and sharing of illegal or harmful content. Platforms must then take steps, based on the information in these assessments, to comply with their duties to protect users from illegal or harmful content. These duties are set out in Table 1.

The draft Bill would also require Ofcom to produce codes of practice that set out "recommended steps" to help platforms comply with their new duties. These steps will not be mandatory, but any alternative approaches taken by platforms must deliver an at least equivalent level of protection for users.

Source: Draft Online Safety Bill, Sections 41 and 45–47 (definitions of illegal and harmful content); Section 26 (assessment about access by children) and Schedule 4 (categories of regulated services); Section 7 (risk assessments for user-to-user services); and Sections 29 and 36 (codes of practice).

## *Regulating legal but harmful content*

34. The Minister told us that regulating legal but harmful content presented the challenge of striking a balance between respecting free speech and ensuring abusive content which falls below the criminal threshold is nonetheless "properly dealt with". He suggested the approach taken in the draft Bill—with companies retaining the power to set their own terms of service, but with regulatory oversight of their enforcement of those rules—addressed the need for that balance.[92]

35. In contrast to the Minister's position, Ruth Smeeth from Index on Censorship argued that "freedom of speech is a fundamental freedom" and that there should not be different sets of rules for online and offline speech.[93] An e-petition started in December 2021 claimed that the powers in the Bill to require social media companies to act on lawful speech the Government defines as harmful were an unacceptable threat to free speech; the petition called for the removal of provisions relating to legal speech from the Bill.[94]

92 Q131
93 Q27; Q24
94 e-petition 601932, Do not restrict our right to freedom of expression online

Concerns about the impact of the inclusion of legal but harmful content in the scope of the draft Bill on freedom of speech online have also been raised by the House of Lords Communications and Digital Committee.[95]

36. Other witnesses to our inquiry did not believe that including legal but harmful content in the legislation was a disproportionate interference with free speech, and told us this might in fact be a way to promote freedom of expression online. Chara Bakalis of Oxford Brookes University argued "we cannot treat [the online and offline worlds] the same", pointing to differences that justified setting different limits on free speech, including the permanency, searchability and speed of dissemination associated with online content; Dr Joe Mulhall from HOPE not Hate also noted the greater ease with which individuals can be targeted for abuse online.[96] Andy Burrows from the NSPCC suggested limiting individuals' exposure to abuse was in fact a prerequisite for freedom of expression and participation online among many communities;[97] Dr Mulhall likewise argued:

> If we address "legal but harmful" properly, we can vastly expand the amount of free speech on online platforms. We have a wide range of people whose freedom of speech is already suppressed: women, LGBT people, people of colour […] We have such toxic online spaces that there are whole areas of the internet where people do not feel comfortable raising their voice and cannot be heard or would be shouted down if they did.[98]

37. We heard different perspectives from witnesses on the appropriateness of the definition of harm used in the draft Bill and how this would affect the potential for legal abuse to be addressed under the legislation.[99] Nancy Kelley from Stonewall indicated she was "broadly happy" with the definition used.[100] Dr Mulhall noted the definition would likely cover content that is legal but nonetheless "very extreme", such as Holocaust denial; he suggested the Bill could not be effective if it focused only on illegal content.[101] By contrast, Ruth Smeeth argued the proposed definition was "very poor", and not properly defined.[102] Matthew Harrison from Mencap suggested the definition contained ambiguities as a result of factors including the option for content to be designated as harmful via secondary legislation at a later stage.[103]

38. **It is appropriate for legal but harmful content to be included in the scope of the Online Safety Bill. The balance of evidence we heard suggests that it is necessary to address this content in the Bill to help protect people from online abuse and promote free speech among groups currently unable to fully express themselves online. However, the lack of clarity in the draft version of the Bill on what content will be covered under this definition is unhelpful. Providing greater clarity on the scope and scale of content the Government expects this definition to capture, and reducing reliance on Ministerial powers to designate such content via secondary legislation at a later date, would be more consistent with respect for freedom of expression.** ***We recommend that***

95 Communications and Digital Committee, First Report of Session 2021–22, Free for all? Freedom of expression in the digital age, HL Paper 54, para 182
96 Q25 [Chara Bakalis]; Q25 [Dr Mulhall]
97 Q55 [Andy Burrows]
98 Q28 [Dr Mulhall]
99 See Box 5 for the definition of harmful content used in the Bill
100 Q13
101 Q28 [Dr Mulhall]; Q37 [Dr Mulhall]
102 Q24; Q39 [Ruth Smeeth]
103 Q4 [Matthew Harrison]

***the Online Safety Bill should include as comprehensive an indication as possible of what content will be covered under its provisions on content that is harmful to adults or to children in the primary legislation.***

## Communities disproportionately targeted online

39. We heard that the link between certain characteristics a person may possess (such as their disability, sexuality, ethnic background or gender) and the risk of facing online abuse[104] means that it is important for the Online Safety Bill to link in with existing equalities, hate crime and Violence Against Women and Girls (VAWG) legislation. Nancy Kelley argued for "really close inter-relationships" to be made between the Bill and hate crime legislation.[105] Women's Aid stressed that online abuse should be "recognised as a harmful form of domestic abuse and VAWG and must be fully integrated within the existing policy and legal framework for these crimes".[106]

40. The Minister suggested the draft Bill already contained provisions to reflect the abuse faced by people from certain communities—in particular, the provision for the definition of content that is harmful to adults to take into account where content may "particularly affect" people or groups with a certain characteristic.[107] In addition, the Government has also previously indicated that online abuse will be included in the priority illegal and harmful content that will be designated in secondary legislation,[108] and that this will include, for example, racist abuse.[109]

41. Witnesses maintained that the Bill should go further and more directly seek to tackle abuse aimed at individuals or groups most likely to receive such abuse. Seyi Akiwowo from Glitch claimed that the lack of specific protections for sex or gender in communications or hate crime law meant the draft Bill's duties relating to illegal content would have a very limited effect on tackling severe gendered abuse. She told us "we cannot leave it to secondary legislation to look at the gendered nature of online abuse", and proposed that gender-based violence and abuse be explicitly mentioned in the Bill as content platforms must address.[110] She also suggested platforms should have to take into account gender and other equalities when conducting the risk assessments the Bill would require them to undertake.[111] Matthew Harrison argued the protected characteristics in the Equality Act should be explicitly referenced in the Bill, to ensure specific consideration is given to the online safety needs of these users and to provide an important sense of direction to the Bill.[112]

104 See paragraph 14
105 Q13
106 Women's Aid Federation of England (TOA0011)
107 Q160. See also Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Section 46(4)), CP 405, 12 May 2021
108 PQ 11725 [on Social Media: Hate Crime], 11 June 2021. See Box 5 for more information on the Secretary of State's power to designate "priority" illegal or harmful content platforms must address
109 PQ 33294 [on Internet: Racial Discrimination], 19 July 2021
110 Q43 [Seyi Akiwowo]
111 Q46 [Seyi Akiwowo]. See Box 5 for more information on the duty the draft Bill would impose on platforms to carry out risk assessments in relation to illegal or harmful content
112 Q14 [Matthew Harrison]. Nancy Kelley also indicated her support for the Bill "linking […] into" the Equality Act protected characteristics; see Q13

42. Witnesses also felt that the experiences of those receiving online abuse should be carefully considered when responding to the problem. For instance, William Perrin from the Carnegie UK Trust told us it was good practice to take a "victim-led" approach to tackling harms.[113] Seyi Akiwowo told us that groups like Glitch and the NSPCC, who provide support to victims of online abuse, have "a real ear to the ground" on victims' experiences and emerging forms of online abuse, and suggested Ofcom should work closely with these groups in its role as the online safety regulator. She suggested this would help ensure future regulation of online platforms was responsive to the needs of users who are more likely to receive or need protection from abuse.[114]

43. The draft Online Safety Bill would require Ofcom to consult with civil society groups in developing codes of practice for platforms and guidance on platforms' transparency reporting requirements.[115] However, Andy Burrows expressed concern that social media companies would "significantly scale up their policy and their legal teams to try and influence the regulator and its worldview"; he argued that there needed to be stronger user advocacy arrangements, beyond those already outlined in the draft Bill, to ensure a "fair fight" between those companies and groups representing users suffering abuse.[116] The Minister argued the consultation processes on codes of practice "will provide a ready opportunity for people who are affected by this to have their voice heard and their views clearly taken on board",[117] and Orla MacRae from the Department for Digital, Culture, Media and Sport indicated that further duties on Ofcom to establish user advocacy mechanisms would be included in the legislation before it is enacted.[118]

44. **The Government's online safety proposals do not go far enough in acknowledging and seeking to tackle the heightened levels of abuse faced by some communities online. While the requirement for Ofcom to consult with civil society groups in developing elements of the regulatory framework such as codes of practice for platforms is welcome, the Online Safety Bill should ensure specific protections for these communities. The Bill should align with the protections already established in the Equality Act and hate crime laws, and require social media companies to consider the different risks potentially faced by users from these communities on their platforms. It should also include additional user advocacy arrangements over and above those already set out in the draft Bill.**

45. ***We recommend that the Online Safety Bill should include a statutory duty for the Government to consult with civil society organisations representing children and users who are most affected by online abuse on the legislation's ongoing effectiveness at tackling online abuse, and how it could be refined to better achieve this goal. This should include, but need not be limited to, explicitly requiring the Secretary of State to consult with such organisations when reviewing the regulatory framework as set out***

113 Q70. Similarly, Dr Bertie Vidgen of the Alan Turing Institute suggested people affected by abuse should have "a much bigger voice and a much bigger role" in the policy and civic discourse on this issue; see Q75 [Dr Vidgen]

114 Q51

115 Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Sections 29(5)(e) and 50(2)(e)), CP 405, 12 May 2021. See Box 5 for more information on codes of practice and Box 2 for more information on platforms' transparency reporting requirements.

116 Q46 [Andy Burrows]

117 Q143 [Chris Philp]

118 Q143 [Orla MacRae]

***in Section 115 of the draft Bill. The organisations consulted in this way should include those consulted by Ofcom in developing codes of practice and transparency reporting guidance for platforms.***

46. ***We recommend that the Online Safety Bill should include abuse based on the characteristics protected under the Equality Act and hate crime legislation as priority harmful content in the primary legislation. It should also list hate crime and Violence Against Women and Girls offences as specific relevant offences within the scope of the Bill's illegal content safety duties and specify the particular offences covered under these headings, as the draft Bill already does for terrorism and Child Sexual Exploitation and Abuse offences.***

47. ***The risk assessments platforms will be required to carry out under the new online safety regulatory framework must not treat all users as being equally at risk from abusive content or behaviour. Instead, we recommend that platforms should be required to give separate consideration to the different risks faced by groups including women, users from minority ethnic backgrounds, disabled users, and LGBT+ users, and that this requirement should be made explicit in the risk assessment duties set out in the Online Safety Bill.***

## Protecting children from harmful content

48. We heard concerning evidence about the scale of children and young people's exposure to abusive content online. The NSPCC told us that 33% of children aged 11 to 18 have reported seeing the bullying of others online.[119] In all of the school engagement sessions that we attended, students reported to us that they feel that seeing abuse is just part of the online experience.[120] The Minister told us that the Online Safety Bill would place an "absolute obligation" on social media platforms to actively prevent children accessing content harmful to them, even if this content is not illegal or prohibited under their terms and conditions; he suggested this would mean, for example, that it would be "generally prohibited" for a platform's content recommendation algorithms to promote such material.[121] Theo Bertram from TikTok suggested the Bill enshrines the principle that social media companies should be making their platforms safer by design for children.[122]

49. As set out in Box 5 and Table 1 above, only platforms which meet the "child user condition" set out in the Bill will be required to comply with the duties to protect children from content harmful to them on the platform. Andy Burrows argued the child user condition proposed in the draft Bill—which would be met if a platform has, or is likely to attract, a "significant number" of child users[123]—sets too high a threshold and would allow harmful content to continue to proliferate on platforms excluded from the scope of these duties, leading to harm being "displaced" rather than tackled.[124] We note that

119 National Society for the Prevention of Cruelty to Children (TOA0019)
120 See Annex: Summary of school engagement
121 Q131; Q136
122 Q111
123 Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Section 26), CP 405, 12 May 2021
124 Q43 [Andy Burrows]

the Joint Committee on the Draft Online Safety Bill has also recommended[125] that the child user condition in the Bill should be the same as the test underpinning the ICO Age Appropriate Design Code.[126]

50. **It is not acceptable that young people should see encountering abuse as just part of the online experience. We welcome the strength of the duties the draft Online Safety Bill would impose on platforms to help reduce the chance that children and young people will come across or be targeted by abusive content online. However, we are concerned that the draft Bill's chosen threshold for the child user condition may mean children will remain at risk of encountering abusive and other harmful content on smaller platforms, where it can still lead to real-world harm.**

51. ***The Government must ensure the Online Safety Bill's safety duties relating to content harmful to children apply across a sufficiently comprehensive range of platforms to prevent young people continuing to be able to access or encounter abusive or other harmful content online once the legislation is enacted. We recommend that the Government reviews the child user condition proposed in the draft Bill to ensure it does not impede this aim by excluding too many platforms from the scope of these duties.***

## Protecting adults from harmful content

### *Scope of the proposed duties*

52. Under the draft Online Safety Bill, content that is legal but harmful to adults would only be in scope of the legislation if it was hosted on the largest "category 1" platforms.[127] However, witnesses highlighted that abuse faced by adults online is not confined to the largest platforms. Danny Stone from the Antisemitism Policy Trust argued that "some so-called alternative platforms, smaller platforms, are designed for harm, and some of them have significant levels of abuse", including legal content such as Holocaust denial.[128] Seyi Akiwowo claimed that women are often targeted for abuse "on niche platforms—platforms that are meant to be about parenting, animals or animal rights, but are being used to dox people's personal information to troll them".[129] We heard no evidence to suggest that the negative effects of this abuse on people's wellbeing or freedom of expression were any less simply because this behaviour occurred on a smaller platform.[130]

53. Nancy Kelley suggested it would be important for the Online Safety Bill to cover content harmful to adults beyond that hosted on the largest platforms:

> What we know from our community is that much of this hate [faced by LGBTQ+ people online] is fomented on smaller platforms that would be

125 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, para 211

126 The ICO (Information Commissioner's Office) Age Appropriate Design Code sets standards in relation to in-scope online services' obligations to protect children's data online. See: ICO, Introduction to the Age appropriate design code (accessed 18 January 2022)

127 See Box 5 and Table 1 above. See also Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Schedule 4), CP 405, 12 May 2021

128 Q2 [Danny Stone]

129 Q42 [Seyi Akiwowo]

130 See paragraphs 16–17 and 36 for more information on these negative effects

> completely unregulated under the current scheme. Regulation would need to be appropriate to the size and nature of the platform, but to leave that space untouched in terms of legal but harmful content is a major loophole.[131]

In response to this point, the Minister indicated the Government was considering whether to amend the conditions for a platform to be classed as Category 1 to cover platforms with either a high number of users or a high risk of harm to users—rather than requiring both conditions to be met, as is currently the case in the draft Bill.[132]

54. **Abusive content hosted on smaller platforms can play a significant role in helping to encourage prejudicial attitudes or even real-world harm. Failure to address this content would risk significantly undermining the potential impact of the proposed online safety legislation in tackling online and offline hate. The duties set out in the Online Safety Bill relating to content that is legal but harmful to adults must apply to a wide enough range of platforms to ensure that abusive content is removed from the online sphere, not merely shifted from larger platforms onto smaller ones subject to less regulatory oversight.**

55. ***We recommend that the Online Safety Bill requires smaller (non-category 1) platforms to take steps to protect users from content that is legal but harmful to adults, with a particular focus on ensuring these platforms cannot be used to host content that has the potential to encourage hate or prejudice towards individuals or communities.***

### *Strength of the proposed duties*

56. The draft Online Safety Bill would impose a duty on the largest Category 1 platforms to protect adult users' safety online by requiring them to set and consistently enforce terms of service that specify how content that is legal but harmful to adults is to be "dealt with".[133] The Minister described this as "a huge step forward" compared to the current situation where, he argued (and as we heard from other witnesses), "those terms and conditions are not properly or consistently enforced".[134] Nancy Kelley argued the Bill was right to "emphasise the enforcement side of the picture", suggesting that "just enforcing the standards as they are would be an enormous transformative step forward for the experience of participating for all of us online".[135]

57. We asked the social media companies who gave evidence to us what impact they expected this duty to have in practice. Beyond Theo Bertram's suggestion that the legislation would require platforms to conduct more closely specified risk assessments to identify harmful content, they were unable to tell us in any detail how the proposed duty might change their practices, including how it might affect what content would be covered under their community standards or what action they would take to "deal with" harmful content.[136] Katy Minshall from Twitter and Rebecca Stimson from Meta both argued

131 Q4 [Nancy Kelley]
132 Q131
133 See Box 5 and Table 1 above. See also Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Section 11), CP 405, 12 May 2021
134 Q152; Q131
135 Q10 [Nancy Kelley]
136 Qq98–104

their platforms' responses would depend on as-yet undefined elements of the regulatory framework, such as the planned codes of practice and the priority harms designated in secondary legislation.[137]

58. The Antisemitism Policy Trust argued in written evidence that "in its current form, we do not have confidence that the duty placed upon category 1 platforms will be fully effective".[138] It called for minimum standards for platforms' responses to harmful content to be set, especially in view of the "inconsistent"[139] terms of service it noted platforms have chosen to set in the past.[140] William Perrin likewise argued that this duty was "extremely weak". To effectively tackle abuse, he suggested the process of platforms setting their terms of service needs to be:

> Much more driven by regulatory and civil society interrogation. It must not just be, "So we set out what we are doing in our terms and conditions, and that is ok." There needs to be a process that assesses whether that is effective in mitigating or preventing harms.[141]

59. William Perrin also suggested that to effectively tackle harmful content would require looking beyond platforms' compliance with their terms of service and the effectiveness of their content moderation processes. Instead, he argued there should be a greater focus on giving Ofcom "a stronger ability […] to drive through" actions by platforms to mitigate or prevent the risks of harm to users found in their risk assessments, including risks arising from content that is legal but harmful to adults.[142] We also note that football organisations drew attention, in their written evidence to the Joint Committee on the Draft Online Safety Bill, to the very limited scope the duty set out in the draft Bill provides for Ofcom to intervene if it feels platforms are failing to effectively protect adult users from the risk of harm arising from legal content.[143]

60. **The Online Safety Bill should retain the provision in the draft Bill to hold platforms liable for failing to consistently enforce their terms of service. We heard that this step would significantly improve users' online experiences—especially those users most likely to face abuse. However, compliance with rules that platforms themselves retain the freedom to set does not provide a sufficiently clear, objective or robust standard of expected protection for adult users in relation to content that is legal but harmful. The Bill should provide a stronger framework in primary legislation for tackling the harm arising from this content.**

## Encouraging safety by design

61. Witnesses told us that tackling online abuse does not just mean platforms having rules in place to allow abusive or hateful content to be removed once it has been posted, but also ensuring platforms minimise the chance for that content to be posted, shared and amplified on the platform in the first place. For example, Ellen Judson from the

137 Q98 [Rebecca Stimson]; Q104 [Katy Minshall]
138 Antisemitism Policy Trust (TOA0008)
139 Antisemitism Policy Trust (TOA0008)
140 As noted above, Danny Stone from the charity raised concern some platforms were "designed for harm" in the content they allow to be posted. See paragraph 52
141 Q66
142 See Q69. We explore this suggestion in more detail in the following section; see paragraphs 61–63
143 The Football Association, The Premier League, EFL, and Kick It Out, Written evidence to the Joint Committee on the Draft Online Safety Bill, HC 609, OSB0007

think tank Demos suggested the "post hoc" nature of content moderation means it is an inherently limited response to online abuse, and suggested platforms should be "proactive" and design their systems in ways that reduce the risk that this content will be able to cause harm to users to begin with.[144] Steps we heard platforms could take in line with this approach include changes to the algorithms used to recommend content and create newsfeeds or timelines, to reduce their propensity to promote abusive or harmful content;[145] and cooling-off periods for newly created accounts to discourage the use of "throwaway" accounts.[146]

62. We heard the Online Safety Bill could go further in encouraging platforms to change how their systems are designed to help tackle abuse and promote user safety. Ellen Judson highlighted that there are elements in the draft Bill that focus on system design,[147] but suggested these were "secondary" to a focus on content moderation. She told us this was especially the case in relation to content that is legal but harmful to adults, where the duty on platforms is framed exclusively in terms of enforcement of platforms' terms of service (rather than mitigating and managing the risks of harm to users—as is the case with the duties relating to illegal content and content harmful to children).[148] She argued there was a need to consider how platform design issues "could be brought more to the front of the duties" in the Bill.[149]

63. A common suggestion from witnesses on how the Online Safety Bill could put greater emphasis on safety by design approaches—especially in relation to legal content harmful to adults—was to place an explicit statutory duty on platforms to protect users from reasonably foreseeable risks of harm. Some witnesses characterised this as a "foundational" duty,[150] which could underpin the specific duties relating to illegal or harmful content. William Perrin suggested a duty of this kind was necessary as the question of what content is deemed acceptable or not under platforms' rules was "a downstream issue that arises long after you have taken design decisions".[151] Danny Stone argued this change would give Ofcom more scope to focus "on the systems that are enabling harmful content to be spread", rather than just platforms' responses to that content once they become aware of it.[152] The idea of a foundational duty was also supported by Andy Burrows, Nancy Kelley and Stephen Kinsella.[153]

144 Q61. Dr Bertie Vidgen from the Alan Turing Institute and Katy Minshall both also argued it is necessary to look beyond content moderation and towards system design to tackle abusive behaviour online; see Q60 [Dr Vidgen]; Q105 [Katy Minshall]

145 See, for example, Q61 [Ellen Judson]

146 Q54 [Andy Burrows]; Q61 [Ellen Judson]

147 For example, she pointed to mentions in the Bill for "algorithms […] platform design, and business models"; see Q62. The draft Bill would require platforms to consider "how the design and operation of the service (including the business model, governance and other systems and processes)" may affect the risks users face on the platform, and how the platform's content recommendation algorithms may affect the risk of users encountering harmful or illegal content on the platform, when conducting the illegal and harmful content risk assessments mandated in the Bill. See Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Section 7), CP 405, 12 May 2021

148 Q62

149 Q62

150 This term was used by witnesses including Danny Stone (Q3), Andy Burrows (Q50) and William Perrin (Q64)

151 Q64

152 Q4 [Danny Stone]

153 Q50 [Andy Burrows]; Q11 [Nancy Kelley]; Q50 [Stephen Kinsella]

64. We also heard that to properly hold social media companies to account for how their platform design choices affect user safety, and to help identify optimal safety by design approaches, greater data transparency by platforms and powers for Ofcom to interrogate platforms' internal data would be needed. Ellen Judson argued there was a systemic evidence gap around how changes platforms have made to their features or functionalities have affected the potential for harm:

> Platforms are doing these kinds of tests. They are tweaking things like the algorithmic systems. They are making design changes. Twitter increased its character count. Did that have any effect on abuse? I do not know, but I feel like that is the kind of question that we would want the regulator to be able to ask.[154]

65. Danny Stone also pointed to the importance of access to platforms' data in building a good understanding of the harms users experience and how these can best be counteracted; he welcomed the duty in the draft Bill on platforms to produce transparency reports[155] as important to help achieve this.[156] Katy Minshall highlighted that researchers can already access Twitter data via the platform's Application Programming Interfaces.[157]

66. **The Government's regulatory proposals should encourage social media companies to prevent or reduce the risk of users being harmed by abusive and hateful content in the first place, not just remove or otherwise deal with such content as it arises. However, the draft Online Safety Bill gives Ofcom very limited scope to ensure platforms are taking positive steps to protect adult users from this risk where abuse falls below the criminal threshold. Where content has been identified as harmful, users should be able to expect platforms to take proportionate steps to proactively protect their safety and wellbeing, and the regulator should be able to ensure this expectation is being met.**

67. ***We support calls for the Online Safety Bill to include a foundational duty on platforms to protect users from reasonably foreseeable risks of harm identified in their risk assessments, including harm arising from abusive content that is legal but harmful to adults. We recommend that this should include an explicit expectation that platforms consider how not only content moderation, but also changes to system design and user functionalities, could help mitigate or prevent these risks.***

154 Q61
155 See Department for Digital, Culture, Media and Sport, Draft Online Safety Bill (Section 49), CP 405, 12 May 2021
156 Q4 [Danny Stone]
157 Q128. See Twitter, About Twitter's APIs (accessed 18 January 2022)

# 5 Online abuse and the criminal law

## The current situation and calls for change

68. Existing criminal offences can cover abusive online content such as death threats or harassment. Offences which address Violence Against Women and Girls (VAWG) can also be applied where this behaviour is perpetrated online, for example engaging in stalking or controlling or coercive behaviour via social media. In addition, specific communications offences prohibit the sending of "indecent" or "grossly offensive" messages online. Criminally abusive online content may also be classed as a hate crime offence if there is evidence that the victim's race, religion, disability, sexual orientation or transgender identity was a factor. There are separate "racially or religiously aggravated" versions of some offences (such as harassment), while a sentence for other offences may be uplifted when there is evidence that the offence was motivated by "hostility" towards the victim on the grounds of one of these characteristics.[158]

69. Our predecessor Committee's report on online abuse and the experience of disabled people concluded that "the current law on online abuse is not fit for purpose". It raised concerns about abusive content or behaviour not being covered under existing laws, and the lack of aggravated offences in relation to disability hate crime. It also concluded that abuse of disabled people online was "under-prosecuted".[159]

70. We heard that offences relating to online abuse remain inadequate and under-enforced. Matthew Harrison from Mencap suggested the picture of under-prosecution of hate speech and abuse found in our predecessor Committee's report "has not changed for disabled people".[160] Danny Stone of the Antisemitism Policy Trust likewise stated "there is not as good a prosecution of antisemitic hate crime as we would like to see".[161] Petitioner Katie Price told us about her experience of reporting abuse aimed at her son Harvey to the police; she suggested this had resulted in very little law enforcement action because "there is nothing in place" to allow perpetrators to be prosecuted.[162] Bobby Norris felt the current law excluded too much abusive content from the scope of prosecution, suggesting the legal threshold of "grossly offensive" was much higher than what many people considered offensive in practice.[163]

71. A popular recent e-petition suggested the law was also over-criminalising online speech in some cases, with negative implications for online freedom of expression.[164] The petition, which attracted over 20,000 signatures before closing in October 2021, pointed to the lack of clarity in the legal definition of "grossly offensive" content and suggested that this had led to prosecutions and convictions for "jokes and petty arguments" online. The Government's response to the petition stated its commitment to "upholding rights to freedom of expression" and acknowledged petitioners' concern about the vagueness of the

158 Information about possible criminal offences arising from online communications can be found at: Crown Prosecution Service, Social Media - Guidelines on prosecuting cases involving communications sent via social media (accessed 18 January 2022)

159 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, para 31

160 Q20

161 Q21 [Danny Stone]

162 Q24 [Katie Price]; Q42

163 Q3

164 e-petition 582423, Repeal Section 127 of the Communications Act 2003 and expunge all convictions

term "grossly offensive". It pointed to the Law Commission's then-ongoing review of laws related to harmful and abusive communications online and indicated it would "carefully consider" possible changes to the law following the publication of the Commission's final recommendations.[165]

## Proposed reforms to relevant offences

### *Communications offences*

72. As part of our inquiry, we heard from Professor Penney Lewis and Dr Nicholas Hoggard, who led the Law Commission's review of communications offences.[166] They told us their review had concluded there was a need to tackle the "vagueness" of existing offences by framing them in terms of the harm a communication may cause to those who see it, rather than relying on terms such as "grossly offensive" or "indecent".[167] The Commission's July 2021 report recommended the creation of new offences, including a "harm-based" offence and an offence covering threatening communications. The former would criminalise communications "likely to cause harm to a likely audience", with harm defined as "psychological harm, amounting at least to serious distress".[168] The latter would criminalise communications that convey "a threat of serious harm" such as grievous bodily harm or rape.[169] In evidence to the Joint Committee on the Draft Online Safety Bill, the Secretary of State for Digital, Culture, Media and Sport, Rt Hon Nadine Dorries MP, indicated that the Government is "minded" to introduce these proposed offences.[170]

73. We heard that these proposed new offences would have advantages over the existing law. Professor Lewis suggested focusing on the harm caused by a communication, rather than the nature of its content, would make the qualification of free speech rights imposed by the law in this area more proportionate.[171] Dr Hoggard suggested the proposed harm-based offence would better recognise contexts where a harmful communication is not inherently offensive or indecent, such as a domestic abuse perpetrator sending their former partner an image of their new address.[172] He suggested this would be especially helpful in helping to improve the legal response to forms of online Violence Against Women and Girls such as coercive controlling behaviour. We also heard that if the proposed new offences were introduced, some abusive content may be treated as "a more serious offence with a more serious penalty" than if it were prosecuted under existing law.[173]

74. Witnesses we heard from were broadly supportive of the Law Commission's proposals.[174] However, the evidence we heard did not conclusively suggest the reforms would enable more online abuse to be prosecuted, as petitioners Katie Price and Bobby

165 Department for Digital, Culture, Media and Sport, response to e-petition 582423, 21 May 2021
166 Law Commission, Reform of the Communications Offences (accessed 18 January 2022)
167 Q78
168 Law Commission, Modernising Communications Offences, Recommendation 1 (p224), 20 July 2021 (accessed 18 January 2022)
169 Law Commission, Modernising Communications Offences, Recommendation 5 (p226), 20 July 2021 (accessed 18 January 2022)
170 Oral evidence taken before the Joint Committee on the Draft Online Safety Bill on 4 November 2021, HC 609, Q278 [Nadine Dorries]
171 Q78
172 Qq78–79
173 Q80 [Dr Hoggard]; Q82 [Penney Lewis]
174 For example, Dr Joe Mulhall argued the shift towards a focus on harm was "positive", while Matthew Harrison said the proposals were a move "in the right direction". See Q35 [Dr Mulhall]; and Q4 [Matthew Harrison]

Norris wanted to see happen:[175] Professor Lewis told us the Commission's proposals were "better targeted" than existing offences, but that this was not "as simple as saying that there will be more prosecutions". She suggested the focus should not be on a "numbers game" of increasing prosecutions but instead ensuring "the right prosecutions".[176] Similarly, Dr Hoggard stressed that the proposals were not simply intended to make more online content illegal, but rather to refocus the law on culpability and harm, including removing communications where there is no culpability or potential for harm from its scope.[177]

75. Chara Bakalis of Oxford Brookes University questioned whether the proposed harm-based offence was indeed better targeted than current offences. She argued the offence is "too vague and too broad" in defining harm to recipients of abuse in terms of psychological harm when there was limited evidence of the potential for such harm from a one-off communication (as opposed to a series of messages)—thereby posing freedom of expression problems, but also potentially under-protecting victims by reducing the scope for it to be used.[178]

76. The social media companies we heard from raised concerns about how the harm-based offence would intersect with the requirement in the draft Online Safety Bill for them to remove illegal content from their platforms. They cited the difficulty of determining intent or distress, as well as the context-specific nature of some of the posts that it might criminalise.[179] Theo Bertram from TikTok argued enforcing this offence online would require increased guidance and advice from law enforcement to social media platforms, to avoid, as Rebecca Stimson from Meta put it, "putting private companies in the position of working out what is crime and what is not".[180]

77. **The Law Commission is right to recommend refocusing online communications offences onto the harm abusive messages can cause to victims. We welcome the Government's commitment to adopt the proposed threatening and 'harm-based' communications offences. However, we also acknowledge the uncertainty and hesitation of some witnesses about how the new harm-based offence will be interpreted in practice, including the role of social media companies and other online platforms in identifying this content—as well as other witnesses' desire for the law to deal with more cases of online abuse more strongly.**

78. ***The Government should monitor how effectively any new communications offences that are enacted—in particular, the Law Commission's proposed harm-based offence—protect people from, and provide redress for victims of, online abuse, while also respecting freedom of expression online. We recommend that the Government publishes an initial review of the workings and impact of any new communications offences within the first two years after they come into force.***

175 See paragraph 70
176 Q81
177 Q85 [Dr Hoggard]
178 Qq31–32
179 Q98 [Rebecca Stimson]; Q130 [Theo Bertram]
180 Q130 [Theo Bertram]; Q130 [Rebecca Stimson]

### *Hate crime*

79. The Law Commission has also recently concluded a review of hate crime laws. It published a consultation paper as part of this review in September 2020; the Commission's final recommendations were published in December 2021.[181] Professor Lewis, who also oversaw this review, told us that hate crime law was a key way in which the criminal law could acknowledge and respond to the disproportionate targeting of online abuse towards specific communities.[182] We heard that online hate crime is rising: Matthew Harrison pointed to evidence from charities Leonard Cheshire and United Response that online disability hate crime had increased by 52% in 2020/21,[183] while Nancy Kelley from Stonewall cited research showing an international rise in online hate speech against LGBT+ people.[184]

80. The Law Commission's final recommendations acknowledged two points highlighted in our predecessor Committee's 2019 report: firstly, the unequal treatment of protected characteristics in hate crime law;[185] and secondly, the failure to classify abuse of disabled people as a hate crime in cases where the offence may have been motivated by a sense that disabled people are easy targets, rather than being clearly motivated by "hostility".[186] The Commission recommended extending existing aggravated hate crime offences to cover not just race and religion but rather all characteristics currently protected under hate crime law, in line with our predecessor Committee's recommendation to ensure disability hate crime has parity with other hate crime offences.[187] The Commission also recommended reforming the motivation test for an offence to be treated as a hate crime, proposing an alternate test of motivation on the grounds of "hostility *or prejudice*".[188]

81. **We support the proposals in the Law Commission's hate crime review to extend aggravated hate crime offences across all characteristics protected under existing hate crime legislation, and to reform the 'hostility' motivation test to better reflect the nature of some hate crimes affecting disabled people—both of which were called for in the previous Petitions Committee's 2019 report, Online abuse and the experience of disabled people.**

82. ***We recommend that the Government accepts the Law Commission's proposals to extend the characteristics to which aggravated hate crime offences can apply, and to reform the motivation test for hate crimes to include prejudice as well as hostility; and that it sets a timeline for bringing these changes forward.***

181 Law Commission, Hate Crime (accessed 18 January 2022)

182 Q91 [Penney Lewis]

183 Q2 [Matthew Harrison]. See Leonard Cheshire, Lockdowns trigger surge in disability hate crime, 6 October 2021 (accessed 18 January 2022)

184 Q21 [Nancy Kelley]

185 See Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 105–107 (relating to inequalities between protected characteristics in hate crime legislation)

186 Professor Lewis told us the Law Commission had heard that the hostility test for hate crime offences "fails to capture the kind of disdainful, contemptuous attitudes that characterise offending against people with disabilities", and that including prejudice as an alternative motivating factor would help capture exploitative behaviour such as "mate crime", which was also highlighted as a problem in our predecessor Committee's 2019 report. See Q92 for Professor Lewis' evidence. See also Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 110–112 (relating to issues with the hostility motivation condition) and paras 138–148 (relating to online exploitation and "mate crime")

187 Law Commission, Hate Crime Laws, Recommendation 12 (p539), 6 December 2021 (accessed 18 January 2022)

188 Law Commission, Hate Crime Laws, Recommendation 20 (p541), 6 December 2021 (accessed 18 January 2022)

## Enforcing the criminal law

83. We heard from Ruth Smeeth of Index on Censorship that changes to the law risked being irrelevant if they are not backed up with the capacity to enforce these offences, and that this would require dedicating resources to the criminal justice system.[189] The need for additional resources to be put into law enforcement was a common theme in the evidence we heard. Dr Joe Mulhall from HOPE not Hate argued that while specialist units such as the Online Hate Crime Hub do remarkable work to trace individuals posting abusive and hateful speech online, these teams were under-resourced, suggesting the Online Hate Crime Hub consisted of "about three people".[190] Concerns about under-resourcing of the police were also raised by Danny Stone and Matthew Harrison,[191] and both the Joint Committee on the Draft Online Safety Bill[192] and the House of Lords Communications and Digital Committee[193] have concluded that the police and courts require more resources to enforce the law online—especially if the Law Commission's new offences are adopted.[194]

84. We were told that ensuring an effective response to online hate crime would also require addressing the under-reporting of online hate speech.[195] Our predecessor Committee's 2019 report found that many disabled people had "largely or wholly negative" experiences with the criminal justice system, and recommended the Government review how disabled people can be effectively supported when reporting online hate crimes.[196] During our current inquiry we again heard it was vital that victims of disability, LGBT and other hate crimes feel comfortable coming forward to report incidents,[197] and the role of adequate training for police officers to achieve this was again raised.[198] Women's Aid raised similar points regarding online Violence Against Women and Girls offences.[199]

85. **Improvements in the drafting of the criminal law are irrelevant if these offences are not enforced. Many witnesses suggested the police did not have the resources they needed to be able to effectively investigate online abuse and hate crime. This undermines the important role played by the criminal law as a response to abusive behaviour online.**

86. ***Alongside the introduction of the new communications offences, we recommend that the Government ensures the police and other law enforcement bodies have adequate resources to effectively investigate and prosecute communications, hate crime, and Violence Against Women and Girls offences committed online. This should include scaling up the work of existing specialist teams such as the Online Hate Crime Hub.***

189 Q35 [Ruth Smeeth]
190 Q29 [Dr Mulhall]
191 Q21 [Danny Stone]; Q21 [Matthew Harrison]
192 Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 137–138
193 Communications and Digital Committee, First Report of Session 2021–22, Free for all? Freedom of expression in the digital age, HL Paper 54, para 123
194 The Home Affairs Committee has also previously called for extra police funding to ensure the police remain able to fulfil their duties in the context of challenges including "an explosion of internet crime, with the evidential challenges that creates". See Home Affairs Committee, Tenth Report of Session 2017–19, Policing for the future, HC [2017–19] 515, para 165
195 See paragraph 18 for details of the evidence we heard on under-reporting of online hate crimes
196 Petitions Committee, First Report of Session 2017–19, Online abuse and the experience of disabled people, HC [2017–19] 759, paras 135–136
197 See for instance, Q19 [Nancy Kelley]
198 Q19 [Nancy Kelley]; Q20 [Matthew Harrison]
199 Women's Aid Federation of England (TOA0011)

***The Government should also ensure police officers are being offered the right training to identify when these offences have been committed and to support victims of these offences when they come forward.***

# 6 Anonymity and accountability

## The risks and value of online anonymity

87. The petitions that prompted our inquiry both raised concerns that social media users were not being held accountable for their actions online.[200] Many social media platforms allow users to operate anonymous accounts that are unrelated to their real name, which has been suggested as one factor driving this perceived lack of accountability: Katie Price's petition explicitly called for the removal of online anonymity to reduce abusive behaviour online and help ensure abusive users can be traced by the police. A previous e-petition specifically calling for a ban on anonymous accounts on social media, "to stop trolls abusing people without any consequences", received almost 17,000 signatures between July 2020 and January 2021.[201] Over the course of our inquiry, online anonymity emerged as a key issue not only for our work but also in wider public and policy discussions of online abuse.[202]

88. Danny Stone from the Antisemitism Policy Trust argued the ability to post anonymously enables abusive behaviour, and pointed to research suggesting disinhibition effects from anonymity can lead to increased hateful behaviour; he cited a figure of 40% of online antisemitic incidents in a reference month arising from anonymous accounts.[203] Nancy Kelley from Stonewall, and Stephen Kinsella from campaign group Clean Up The Internet, argued evidence suggested anonymity should be seen as a factor that increases the risk of users posting abuse and other harmful content.[204] Danny Stone and Stephen Kinsella both suggested anonymity should be seen as a risk factor platforms should be required to address in their risk assessments under the new online safety regulatory framework.[205]

89. Other witnesses suggested that evidence of a connection between anonymity and abusive behaviour was weak or unclear. Ruth Smeeth from Index on Censorship told us that the majority of abuse she had personally received came from individuals using their own names.[206] Dr Bertie Vidgen from the Alan Turing Institute told us that while there were strong theoretical arguments for a link between anonymity and abusive behaviour that were borne out in qualitative research, this link is less well-established in quantitative studies.[207] Social media companies told us anonymous accounts did not disproportionately drive harm on their platforms.[208]

200 See Boxes 3 and 4
201 e-petition 332315, Ban anonymous accounts on social media
202 For example, the report of the Joint Committee on the Draft Online Safety Bill considered issues around anonymity and traceability; and the Secretary of State for Digital, Culture, Media and Sport has indicated the Government is considering strengthening the Online Safety Bill's provisions on anonymous abuse. See Joint Committee on the Draft Online Safety Bill, Report of Session 2021–22, Draft Online Safety Bill, HC 609, paras 84–94; and Daily Mail, Nadine Dorries reveals the online abuse she has received as she promises tougher laws against web trolls, 22 October 2021 (accessed 18 January 2022)
203 Q6 [Danny Stone]
204 Q6 [Nancy Kelley]; Q44 [Stephen Kinsella]
205 Q44 [Stephen Kinsella]; Q6 [Danny Stone]
206 Q29 [Ruth Smeeth]
207 Q73
208 Q122 [Rebecca Stimson]; Q123 [Theo Bertram]

90. We heard the ability to post anonymously was not the right focus in attempting to resolve the problem of online abuse. Dr Vidgen argued anonymity should not be seen as the single factor driving abusive behaviour online, suggesting it is only one factor among others.[209] Likewise, Chara Bakalis from Oxford Brookes University argued that "focusing so much on anonymity and trying to make people say who they are online" risked misconstruing the problem as a question of some individuals' behaviour, rather than the overall toxicity of online spaces.[210] We also heard that the ability to post anonymously is indispensable for many users: Ruth Smeeth highlighted its value for victims of domestic abuse, while Nancy Kelley highlighted how it can help LGBT+ people "be their full selves" online in a way they cannot offline.[211] Ellen Judson from Demos warned that "there is not a reduction of anonymity that only negatively impacts people who are abusive".[212]

91. Some witnesses argued for responses to anonymous abuse that do not specifically take into account its anonymous nature. Ruth Smeeth suggested that ensuring criminal prosecutions are pursued for online abuse where appropriate, whether or not this abuse is perpetrated anonymously, could lead to cultural change and deter this behaviour.[213] Dr Joe Mulhall from HOPE not Hate suggested platforms should change their content promotion algorithms to reduce the proliferation of harmful content (including content posted anonymously); Dr Vidgen likewise suggested the risks of allowing anonymous posting could be managed if platforms were operating "safe by design" systems.[214]

92. **Anonymous abuse online is significant in both its volume and impact. However, the evidence we heard suggested that tackling the abuse being perpetrated under the cloak of anonymity, rather than imposing restrictions on online anonymity, should be the focus of efforts to resolve this problem. Allowing users to post anonymously does nonetheless entail a risk that this capability is misused, and so it would be sensible and proportionate for online platforms to be required to specifically evaluate—and consider what steps could be taken in response to—links between anonymity and abusive content on their platform.**

93. ***As part of the risk assessments social media platforms will be required to carry out under the new online safety regulation, we recommend that platforms should be required to evaluate the role played by anonymous accounts in creating and disseminating abusive content, and to consider how to minimise the misuse of anonymity for this purpose. Platforms should be required to take action to mitigate risks of harm to users uncovered through this work arising from anonymously posted content.***

## Anonymity or traceability

94. Both Bobby Norris and Katie Price's petitions that prompted this inquiry raised the need to ensure users can be identified and traced so that they cannot evade sanctions for their actions either by social media companies (such as platform suspensions or bans) or by law enforcement. Dr Vidgen told us there was a key distinction between the ability

209 Q74 [Dr Vidgen]
210 Q29 [Chara Bakalis]
211 Q29 [Ruth Smeeth]; Q6 [Nancy Kelley]
212 Q74 [Ellen Judson]. Dr Joe Mulhall from HOPE not Hate told us online anonymity was "too important" to limit, even to reduce the risk of online abuse; see Q29 [Dr Mulhall]
213 Q29 [Ruth Smeeth]
214 Q29 [Dr Mulhall]; Q73 [Dr Vidgen]

to post anonymously, and "traceability", and suggested that acknowledging the benefits of giving users the option to post without publicly identifying themselves did not imply users should be able to escape accountability for their posts.[215]

### *Identifying users on social media platforms*

95. Bobby Norris' petition argued it is "far too easy" for social media users who have been suspended from a platform to get around this sanction by signing up for a new account and continuing to send abuse:

> No sooner have you blocked them than they have gone back online, within five minutes, and started another account. They are not being held accountable. You are forever chasing your tail because you're blocking and they're opening them literally within minutes.[216]

Katie Price and her mother Amy also raised the issue of users returning after previously being banned from a platform.[217]

96. The social media companies we heard from told us they are already able to use "a range of digital forensics" to identify and prevent previously banned users returning to the platform.[218] Dr Mulhall noted that even as a small NGO, HOPE not Hate can trace far-right users' accounts, including identifying previously banned users returning to the platform. He argued that when it came to enforcing platform bans:

> [The platforms] could be doing that themselves if they wanted to put the time and resources to look into accounts that were causing harm, but they do not […] A huge amount of this is about the will of the tech platforms just not being there.[219]

97. **Social media platforms told us they already have rules against previously banned users returning, as well as the tools and data needed to identify users and prevent them starting new accounts. However, the evidence we heard suggests this is not a priority for them, and that some users are taking advantage of poor enforcement of such bans to continue to behave abusively. This is a significant failing by these platforms.**

98. ***Social media platforms must have robust methods in place to trace users posting content that violates the platform's terms of service, and must effectively enforce their own sanctions against such users. We recommend that, as part of the new online safety regulatory framework, social media platforms should be required to demonstrate to Ofcom that they can identify previously banned users seeking to create new accounts and, where a platform's rules prohibit these users from returning to the platform, that the platform is adequately enforcing these rules. Ofcom should have the power to issue fines or take other enforcement action if a platform is unable to demonstrate this.***

215 Q73 [Dr Vidgen]
216 Q4
217 Q24 [Katie Price]; Q58 [Amy Price]
218 Q124 [Theo Bertram]; Q126 [Katy Minshall]; Q127 [Rebecca Stimson]
219 Q30 [Dr Mulhall]

### *Tracing illegal content*

99. Katie Price's 2021 petition drew attention to the need to ensure social media users can be traced in order to face legal sanctions for their online behaviour where appropriate, even if they are posting anonymously. Rebecca Stimson from Meta stressed to us that social media companies already collect and provide information to law enforcement about accounts posting potentially illegal content, and that they hold an enormous amount of such data regardless of whether the content was posted from a publicly identifiable account.[220] In its May 2021 response to Katie Price's petition, the Government stated:

> The police already have a range of legal powers to identify individuals who attempt to use anonymity to escape sanctions for online harms, where the activity is illegal. The government is also working with law enforcement to review whether the current powers are sufficient to tackle illegal anonymous abuse online.[221]

100. In oral evidence to the House of Lords Communications and Digital Committee in April 2021, David Tucker from the College of Policing suggested that an account being publicly anonymous did not necessarily prevent the police being able to trace a user posting potentially illegal content, but that it may mean that "it takes longer to do it". He also suggested the ability to trace users in individual cases was often a question of capacity and resources.[222] Dr Mulhall noted that when HOPE not Hate reports terrorist content to the police, "invariably, those people are found and prosecuted, because they are prioritised, resources are put towards them and they are tracked down"—but that this was not always the case in relation to anonymous abuse, because the police do not have the time and resources needed to treat abusive content with the same priority.[223]

101. The social media companies we heard from drew attention to their existing cooperation with law enforcement, including providing dedicated tools, teams and training to support the effectiveness of their responses to police requests for information about specific accounts or for content to be removed.[224] However, Danny Stone suggested that social media platforms are patchy and inconsistent in their compliance with requests for information to help reveal the identity of abusive users.[225] He suggested existing police powers to demand information from platforms could be underlined or restated in the Online Safety Bill to help ensure more effective legal responses to anonymous abuse.[226]

102. **Where there is a need to trace and investigate accounts posting potentially illegal content, this is usually technically possible even if the account is publicly anonymous. However, the police's ability to trace accounts posting such content at scale is constrained by a lack of resources. This underlines the need for additional law enforcement resourcing as we call for in our recommendations on online abuse and the criminal law. The mixed evidence we heard about social media platforms' cooperation with police requests for such information makes it welcome that the Government has**

220 Q122
221 Department for Digital, Culture, Media and Sport, response to e-petition 575833, 5 May 2021
222 Oral evidence taken before the Communications and Digital Committee on 20 April 2021, Q192
223 Q29 [Dr Mulhall]
224 Q129
225 For example, we note that Twitter's latest Transparency Center data shows it complied with just 33.6% of government (including law enforcement) information requests in the UK between July and December 2020. See Twitter Transparency Center, United Kingdom (accessed 18 January 2022)
226 Q6 [Danny Stone]

**previously indicated it is looking into the powers available to the police to identify users and tackle illegal anonymous abuse online.** ***We recommend that the Government publishes the conclusions of its work to review whether current police powers are sufficient to tackle illegal anonymous abuse online, and that it sets out a timetable for any changes it believes are necessary as a result.***

## Identity verification on social media

103. Bobby Norris and Katie Price both suggested social media platforms should require users to verify their identity by providing an ID document. Bobby suggested this would not only help platforms stop previously banned users setting up new accounts, but could also lead to "a massive decrease in online hate and trolling—if people knew that they were traceable and that their actions would have repercussions".[227] Katie's petition argued that this change would mean abusive users could be "easily identified and reported to the police and punished".[228] However, we heard that improving the traceability of abusive users is at least as much a question of resources and priorities as it is of giving the police and platforms extra information on users' identities.[229]

**Box 6: Students' views on ID requirements for social media**

In our engagement sessions with schools, many students identified positive potential effects of requiring ID for social media accounts, including tracking down perpetrators of online abuse more easily and helping to prevent abuse occurring in the first place. Some students suggested that this could make the online world safer for children in particular, by reducing the likelihood of "catfishing" and preventing underage children from having accounts. Students suggested benefits of such a requirement would include:

- "Make sure that people can't keep setting up new accounts"
- "Prevent people managing to set up fake accounts"
- "As people are more likely to be identified they may not want to put nasty things"

However, across all schools that fed back to us, young people also raised concerns about the proposal. Many young people highlighted data privacy concerns, as well as scepticism about the effectiveness of such a move. For example, they said that:

- "I don't want social media companies to have access to our IDs. This is a privacy issue, and they already have too much information"
- "This would really increase the risk of identity theft"
- "There are ways to bypass it. People could use a fake ID. People can lie, use false info"

Other concerns raised by students included the impact of such a requirement on young people (many said they do not have access to ID and didn't expect to need this until they were 17 or 18) or people from certain socioeconomic groups (due to the cost of obtaining an ID document); and the risk to young people who may want to use social media in secret, such as LGBT+ young people looking to access online support but for whom it's not safe to be "out" at home.

Source: Petitions Committee public engagement sessions with schools (see Annex)

227 Q4
228 e-petition 575833, Make verified ID a requirement for opening a social media account
229 See paragraphs 96 and 100

104. Stephen Kinsella suggested social media platforms should be required to give all their users the option to verify their identity on a voluntary (rather than mandatory) basis, alongside an option to block interactions with unverified accounts. He argued this would reduce individuals' potential exposure to abuse by screening out content posted by unverified accounts. He suggested this would be especially beneficial for users who consider themselves vulnerable to anonymous abuse or are concerned they may be temporarily more likely to receive abuse as a result of public attention.[230]

105. Other witnesses supported the idea of voluntary user identity verification. Dr Vidgen suggested giving people choice about whether they see anonymous content would be a valuable safety by design innovation.[231] Katy Minshall from Twitter pointed to an existing option on the platform for users to turn off notifications triggered by accounts that are new or have not verified an email address or phone number.[232] The Minister, Chris Philp MP, indicated that the Government was "thinking […] very carefully" about proposals to give users choice in whether they see content posted by anonymous unverified accounts.[233]

106. We heard concerns from some witnesses about the impact of introducing user identity verification more widely on social media (on either a voluntary or mandatory basis). Nancy Kelley suggested ID verification could have a "chilling effect" on the participation of LGBT+ people from less supportive backgrounds on social media.[234] Dr Mulhall and Ellen Judson suggested people from marginalised groups, such as young LGBT+ people or undocumented migrants—who may be less able or willing to verify their account for reasons including concerns about their own safety—would be less able to engage and be heard online if users could block interactions with unverified accounts.[235]

107. Matthew Harrison from Mencap raised concerns about the accessibility of identity verification systems for people with learning disabilities, including highlighting lower levels of ownership of most forms of ID among this group. He suggested there should be "discussion about how it actually works for users who are not going on [social media] with the intention of causing harms but could fall foul of the [identity verification] regulations, keeping them from using it". Stephen Kinsella told us that identity verification need not involve a formal ID document and could be done by linking a social media account to, for example, a bank account;[236] however, Matthew Harrison and Nancy Kelley noted this would still present barriers for some learning disabled or LGBT+ users, on the grounds of accessibility, proportionality and security.[237]

108. **While we heard that there is insufficient evidence to determine that anonymity is the main driver of abusive behaviour online, we recognise that a proportion of abusive content comes from anonymous users. Giving users the option to filter out content from accounts that have not provided a form of identity verification, on a voluntary basis, would offer an extra tool that users can use to give themselves an additional layer of protection from abusive content.**

230 Q45; Q53
231 Q73
232 Q121
233 Q162
234 Q6 [Nancy Kelley]
235 Q30 [Dr Mulhall]; Q74 [Ellen Judson]
236 Q56
237 Q6 [Nancy Kelley, Matthew Harrison]; Q7 [Nancy Kelley]

109. ***We recommend that the Government set an expectation that the largest social media platforms should offer users the option to filter content by user verification status and block content from users who have chosen not to verify their account. User verification should not necessarily have to be in the form of an ID document, and we recommend that Ofcom should conduct research to establish possible methods of account verification that offer a robust way to reduce users' exposure to harmful content while also being maximally inclusive and accessible.***

# 7 Social responses to online abuse

110. We heard that social and educational interventions should also play a role in responding to online abuse, to help foster cultural and behaviour change that could prevent people posting abusive content in the first place. Bobby Norris argued, "no child is born a troll […] teaching people from a young age that that is not acceptable and how to use the internet appropriately is the way that we will overcome this".[238] The charity Protection Approaches told us:

> Solutions to online harms and abuse remain too focused upon the online sphere, where dangerous and divisive behaviour is most clearly seen, rather than on the causes of that behaviour […] Online and tech-based efforts to tackle online abuse […] must also be matched by investments in offline activities such as education-based and community-building interventions.[239]

Among the schools we engaged with where students voted on how best to respond to online abuse, anti-prejudice public awareness campaigns and education in schools emerged as the most popular options—above alternative responses such as banning anonymous accounts or automatically removing posts containing potentially offensive content.[240]

**Box 7: Students' views on anti-prejudice public awareness campaigns**

Students identified that anti-prejudice public awareness campaigns might help reduce abusive behaviour online. For example, they said that such campaigns might mean that:

- "People can feel safe being themselves"
- "Trolls could be helped to think before they speak"
- "People who may have not realised are made to care"

However, they also commented that public awareness campaigns may be ignored, ineffective or even counterproductive:

- "There are better solutions and I personally think that people won't change their behaviour anyways."
- "Biggest issue of a public awareness campaign is not everyone sees it"
- "[Campaigns] are easily forgotten"
- "They can produce a defensive response which defeats the purpose and creates further division"

Source: Petitions Committee public engagement sessions with schools (see Annex)

238 Q10
239 Protection Approaches (TOA0018)
240 See Annex: Summary of school engagement

**Box 8: Students' views on lessons about online behaviour in schools**

Many students called for more education about being online from a younger age based on their personal experiences, suggesting that they had already been online for a number of years by the time relevant topics were covered in the curriculum. Students had specific ideas on what education in schools could look like:

- "Teach us how to report and block others. And what to report."
- "I feel like we need to educate children from around the age of 11–12 about the dangers of social media and how to behave correctly online"

As with public awareness campaigns however, students identified that more education in schools might still be ineffective in tackling online abuse. Some students suggested teachers "won't understand" the issues faced by young people online or that advice from teachers is "not what young people listen to". Some argued that education in schools about being online could be led by fellow pupils.

Other students were concerned that using lesson time to teach about online abuse would reduce their learning in other subjects and might affect their performance in exams. Some also felt that the responsibility to educate young people about online behaviour lay with parents or social media platforms rather than schools.

Source: Petitions Committee public engagement sessions with schools (see Annex)

## Digital citizenship and challenging prejudice

111. Some witnesses saw a role for education and campaigns challenging prejudiced attitudes, including among adults, in promoting online behaviour change. Dr Joe Mulhall from HOPE not Hate argued:

> People engage in online hate because they hate people. We have to root our online education in much wider programmes of attempting to deal with hate and discrimination across society.[241]

Theo Bertram from TikTok told us about the platform's #SwipeOutHate campaign ahead of the 2020 European Championships, which he suggested had helped reduce abuse on the platform during the tournament.[242] However, we also heard about the limits of such approaches: Nancy Kelley from Stonewall told us that a small number of "very radicalised" users with prejudiced attitudes towards many communities are responsible for a lot of the online hate faced by many groups, and that a targeted online hate de-radicalisation approach is needed to change the behaviour of these individuals.[243]

112. Other witnesses endorsed the idea of educating social media users in "digital citizenship" and online rights and responsibilities. Seyi Akiwowo from Glitch suggested this should involve ensuring users know about both digital security and how to stay safe online, but also "systemic social norms and values" in the online space and how to support others facing abuse online. She argued this would give users resilience to online harms as new innovations and platforms emerge, and suggested this could be run in a similar way to previous public education campaigns around driving and alcohol.[244] Ruth Smeeth from Index on Censorship suggested community groups such as The Scout Association

241 Q40 [Dr Mulhall]
242 Q110 [Theo Bertram]
243 Q4 [Nancy Kelley]
244 Q55 [Seyi Akiwowo]

and the Women's Institute should be seen as important partners in delivering campaigns of this kind,[245] while Danny Stone from the Antisemitism Policy Trust pointed to the Government's Online Media Literacy Strategy as an important opportunity to deliver digital citizenship education.[246]

113. **Alongside the legal, technological and regulatory responses to online abuse we have considered in this report, there is also a need to achieve long-term cultural and behavioural change that tackles online abuse by discouraging people from posting such content to begin with. The Government's Online Media Literacy programme rightly seeks to give users of online platforms the skills and knowledge they need to be safe online, but there is also an equal need for the Government to invest in programmes which educate both adults and young people about acceptable and supportive online behaviour, and which challenge the prejudiced attitudes which are manifested in online abuse.**

245 Q27; Q40 [Ruth Smeeth]
246 Q11 [Danny Stone]

# Conclusions and recommendations

## The experience of people receiving online abuse

1. Online abuse can have a devastating impact on those who are exposed to it, and we are alarmed at evidence suggesting the problem has worsened since the covid-19 pandemic began. While tackling this issue is important in making the online environment safer for everyone, it must be recognised that online abuse is disproportionately targeted at certain groups. The Government is right to acknowledge the extent of this problem but should assess and track the scale of this behaviour more precisely and comprehensively. (Paragraph 21)

2. *As part of its role as the new online safety regulator, we recommend that Ofcom should regularly report on the incidence of online abuse, illegal hate speech, and Violence Against Women and Girls content on the largest social media platforms. This should include disaggregating estimates of the likelihood of a user encountering or being the target of abusive content according to characteristics including race, disability, sexuality, and gender, as well as differentiating between child and adult users.* (Paragraph 22)

## Social media and user safety

3. Our predecessor Petitions Committee's report concluded that self-regulation of social media had failed. Despite the user safety tools and innovations platforms have introduced since then, these companies have continued to place insufficient priority on user safety to protect users from abusive and hateful behaviour on their platforms, or ensure users are able to effectively raise their concerns when subjected to this behaviour. We support the Government's intention to end social media self-regulation and introduce a statutory regulatory framework. (Paragraph 32)

## The Online Safety Bill

4. It is appropriate for legal but harmful content to be included in the scope of the Online Safety Bill. The balance of evidence we heard suggests that it is necessary to address this content in the Bill to help protect people from online abuse and promote free speech among groups currently unable to fully express themselves online. However, the lack of clarity in the draft version of the Bill on what content will be covered under this definition is unhelpful. Providing greater clarity on the scope and scale of content the Government expects this definition to capture, and reducing reliance on Ministerial powers to designate such content via secondary legislation at a later date, would be more consistent with respect for freedom of expression. *We recommend that the Online Safety Bill should include as comprehensive an indication as possible of what content will be covered under its provisions on content that is harmful to adults or to children in the primary legislation.* (Paragraph 38)

5. The Government's online safety proposals do not go far enough in acknowledging and seeking to tackle the heightened levels of abuse faced by some communities online. While the requirement for Ofcom to consult with civil society groups in

developing elements of the regulatory framework such as codes of practice for platforms is welcome, the Online Safety Bill should ensure specific protections for these communities. The Bill should align with the protections already established in the Equality Act and hate crime laws, and require social media companies to consider the different risks potentially faced by users from these communities on their platforms. It should also include additional user advocacy arrangements over and above those already set out in the draft Bill. (Paragraph 44)

6. *We recommend that the Online Safety Bill should include a statutory duty for the Government to consult with civil society organisations representing children and users who are most affected by online abuse on the legislation's ongoing effectiveness at tackling online abuse, and how it could be refined to better achieve this goal. This should include, but need not be limited to, explicitly requiring the Secretary of State to consult with such organisations when reviewing the regulatory framework as set out in Section 115 of the draft Bill. The organisations consulted in this way should include those consulted by Ofcom in developing codes of practice and transparency reporting guidance for platforms.* (Paragraph 45)

7. *We recommend that the Online Safety Bill should include abuse based on the characteristics protected under the Equality Act and hate crime legislation as priority harmful content in the primary legislation. It should also list hate crime and Violence Against Women and Girls offences as specific relevant offences within the scope of the Bill's illegal content safety duties and specify the particular offences covered under these headings, as the draft Bill already does for terrorism and Child Sexual Exploitation and Abuse offences.* (Paragraph 46)

8. *The risk assessments platforms will be required to carry out under the new online safety regulatory framework must not treat all users as being equally at risk from abusive content or behaviour. Instead, we recommend that platforms should be required to give separate consideration to the different risks faced by groups including women, users from minority ethnic backgrounds, disabled users, and LGBT+ users, and that this requirement should be made explicit in the risk assessment duties set out in the Online Safety Bill.* (Paragraph 47)

9. It is not acceptable that young people should see encountering abuse as just part of the online experience. We welcome the strength of the duties the draft Online Safety Bill would impose on platforms to help reduce the chance that children and young people will come across or be targeted by abusive content online. However, we are concerned that the draft Bill's chosen threshold for the child user condition may mean children will remain at risk of encountering abusive and other harmful content on smaller platforms, where it can still lead to real-world harm. (Paragraph 50)

10. *The Government must ensure the Online Safety Bill's safety duties relating to content harmful to children apply across a sufficiently comprehensive range of platforms to prevent young people continuing to be able to access or encounter abusive or other harmful content online once the legislation is enacted. We recommend that the Government reviews the child user condition proposed in the draft Bill to ensure it does not impede this aim by excluding too many platforms from the scope of these duties.* (Paragraph 51)

11. Abusive content hosted on smaller platforms can play a significant role in helping to encourage prejudicial attitudes or even real-world harm. Failure to address this content would risk significantly undermining the potential impact of the proposed online safety legislation in tackling online and offline hate. The duties set out in the Online Safety Bill relating to content that is legal but harmful to adults must apply to a wide enough range of platforms to ensure that abusive content is removed from the online sphere, not merely shifted from larger platforms onto smaller ones subject to less regulatory oversight. (Paragraph 54)

12. *We recommend that the Online Safety Bill requires smaller (non-category 1) platforms to take steps to protect users from content that is legal but harmful to adults, with a particular focus on ensuring these platforms cannot be used to host content that has the potential to encourage hate or prejudice towards individuals or communities.* (Paragraph 55)

13. The Online Safety Bill should retain the provision in the draft Bill to hold platforms liable for failing to consistently enforce their terms of service. We heard that this step would significantly improve users' online experiences—especially those users most likely to face abuse. However, compliance with rules that platforms themselves retain the freedom to set does not provide a sufficiently clear, objective or robust standard of expected protection for adult users in relation to content that is legal but harmful. The Bill should provide a stronger framework in primary legislation for tackling the harm arising from this content. (Paragraph 60)

14. The Government's regulatory proposals should encourage social media companies to prevent or reduce the risk of users being harmed by abusive and hateful content in the first place, not just remove or otherwise deal with such content as it arises. However, the draft Online Safety Bill gives Ofcom very limited scope to ensure platforms are taking positive steps to protect adult users from this risk where abuse falls below the criminal threshold. Where content has been identified as harmful, users should be able to expect platforms to take proportionate steps to proactively protect their safety and wellbeing, and the regulator should be able to ensure this expectation is being met. (Paragraph 66)

15. *We support calls for the Online Safety Bill to include a foundational duty on platforms to protect users from reasonably foreseeable risks of harm identified in their risk assessments, including harm arising from abusive content that is legal but harmful to adults. We recommend that this should include an explicit expectation that platforms consider how not only content moderation, but also changes to system design and user functionalities, could help mitigate or prevent these risks.* (Paragraph 67)

## Online abuse and the criminal law

16. The Law Commission is right to recommend refocusing online communications offences onto the harm abusive messages can cause to victims. We welcome the Government's commitment to adopt the proposed threatening and 'harm-based' communications offences. However, we also acknowledge the uncertainty and hesitation of some witnesses about how the new harm-based offence will be

interpreted in practice, including the role of social media companies and other online platforms in identifying this content—as well as other witnesses' desire for the law to deal with more cases of online abuse more strongly. (Paragraph 77)

17. *The Government should monitor how effectively any new communications offences that are enacted—in particular, the Law Commission's proposed harm-based offence—protect people from, and provide redress for victims of, online abuse, while also respecting freedom of expression online. We recommend that the Government publishes an initial review of the workings and impact of any new communications offences within the first two years after they come into force.* (Paragraph 78)

18. We support the proposals in the Law Commission's hate crime review to extend aggravated hate crime offences across all characteristics protected under existing hate crime legislation, and to reform the 'hostility' motivation test to better reflect the nature of some hate crimes affecting disabled people—both of which were called for in the previous Petitions Committee's 2019 report, Online abuse and the experience of disabled people. (Paragraph 81)

19. *We recommend that the Government accepts the Law Commission's proposals to extend the characteristics to which aggravated hate crime offences can apply, and to reform the motivation test for hate crimes to include prejudice as well as hostility; and that it sets a timeline for bringing these changes forward.* (Paragraph 82)

20. Improvements in the drafting of the criminal law are irrelevant if these offences are not enforced. Many witnesses suggested the police did not have the resources they needed to be able to effectively investigate online abuse and hate crime. This undermines the important role played by the criminal law as a response to abusive behaviour online. (Paragraph 85)

21. *Alongside the introduction of the new communications offences, we recommend that the Government ensures the police and other law enforcement bodies have adequate resources to effectively investigate and prosecute communications, hate crime, and Violence Against Women and Girls offences committed online. This should include scaling up the work of existing specialist teams such as the Online Hate Crime Hub. The Government should also ensure police officers are being offered the right training to identify when these offences have been committed and to support victims of these offences when they come forward.* (Paragraph 86)

## Anonymity and accountability

22. Anonymous abuse online is significant in both its volume and impact. However, the evidence we heard suggested that tackling the abuse being perpetrated under the cloak of anonymity, rather than imposing restrictions on online anonymity, should be the focus of efforts to resolve this problem. Allowing users to post anonymously does nonetheless entail a risk that this capability is misused, and so it would be sensible and proportionate for online platforms to be required to specifically evaluate—and consider what steps could be taken in response to—links between anonymity and abusive content on their platform. (Paragraph 92)

23. *As part of the risk assessments social media platforms will be required to carry out under the new online safety regulation, we recommend that platforms should be required to evaluate the role played by anonymous accounts in creating and disseminating abusive content, and to consider how to minimise the misuse of anonymity for this purpose. Platforms should be required to take action to mitigate risks of harm to users uncovered through this work arising from anonymously posted content*. (Paragraph 93)

24. Social media platforms told us they already have rules against previously banned users returning, as well as the tools and data needed to identify users and prevent them starting new accounts. However, the evidence we heard suggests this is not a priority for them, and that some users are taking advantage of poor enforcement of such bans to continue to behave abusively. This is a significant failing by these platforms. (Paragraph 97)

25. *Social media platforms must have robust methods in place to trace users posting content that violates the platform's terms of service, and must effectively enforce their own sanctions against such users. We recommend that, as part of the new online safety regulatory framework, social media platforms should be required to demonstrate to Ofcom that they can identify previously banned users seeking to create new accounts and, where a platform's rules prohibit these users from returning to the platform, that the platform is adequately enforcing these rules. Ofcom should have the power to issue fines or take other enforcement action if a platform is unable to demonstrate this*. (Paragraph 98)

26. Where there is a need to trace and investigate accounts posting potentially illegal content, this is usually technically possible even if the account is publicly anonymous. However, the police's ability to trace accounts posting such content at scale is constrained by a lack of resources. This underlines the need for additional law enforcement resourcing as we call for in our recommendations on online abuse and the criminal law. The mixed evidence we heard about social media platforms' cooperation with police requests for such information makes it welcome that the Government has previously indicated it is looking into the powers available to the police to identify users and tackle illegal anonymous abuse online. *We recommend that the Government publishes the conclusions of its work to review whether current police powers are sufficient to tackle illegal anonymous abuse online, and that it sets out a timetable for any changes it believes are necessary as a result*. (Paragraph 102)

27. While we heard that there is insufficient evidence to determine that anonymity is the main driver of abusive behaviour online, we recognise that a proportion of abusive content comes from anonymous users. Giving users the option to filter out content from accounts that have not provided a form of identity verification, on a voluntary basis, would offer an extra tool that users can use to give themselves an additional layer of protection from abusive content. (Paragraph 108)

28. *We recommend that the Government set an expectation that the largest social media platforms should offer users the option to filter content by user verification status and block content from users who have chosen not to verify their account. User verification should not necessarily have to be in the form of an ID document, and*

*we recommend that Ofcom should conduct research to establish possible methods of account verification that offer a robust way to reduce users' exposure to harmful content while also being maximally inclusive and accessible.* (Paragraph 109)

## Social responses to online abuse

29. Alongside the legal, technological and regulatory responses to online abuse we have considered in this report, there is also a need to achieve long-term cultural and behavioural change that tackles online abuse by discouraging people from posting such content to begin with. The Government's Online Media Literacy programme rightly seeks to give users of online platforms the skills and knowledge they need to be safe online, but there is also an equal need for the Government to invest in programmes which educate both adults and young people about acceptable and supportive online behaviour, and which challenge the prejudiced attitudes which are manifested in online abuse. (Paragraph 113)

# Annex: Summary of school engagement

## Background

The Petitions Committee, working with Parliament's Education and Engagement and Select Committee Engagement teams, designed a session to be run in schools during October and November 2021. The session engaged young people in the Committee's inquiry into tackling online abuse. The session asked young people to:

a) Consider how online abuse is currently dealt with by the Government and social media companies;

b) Decide how they thought social media companies and the Government should deal with online abuse;

c) Assess proposals to tackle online abuse and evaluate their advantages and disadvantages;

d) Leave final thoughts on what they thought was most important for the Government to address in tackling online abuse.

The school session was run in at least 12 schools. The session was run with year groups ranging from year 9 (13–14 year-olds) to year 13 (17–18 year-olds). Committee members attended four of the sessions in person or remotely. Students were not selected to be a representative sample of people to feed into the Committee's work.

Eleven of the schools which ran the session sent the students' responses to the Committee, totalling responses from at least 500 young people. The schools that fed back to the Committee were:

a) Armadale Academy, West Lothian (attended by Martyn Day MP)

b) Avon Valley School, Warwickshire

c) De Warenne Academy, Don Valley (attended by Nick Fletcher MP)

d) Framlingham College, Suffolk

e) Gosforth Academy, Newcastle (attended by Catherine McKinnell MP)

f) Graeme High School, Falkirk

g) Grove Academy, Dundee

h) Penyrheol School, Swansea (attended by Tonia Antoniazzi MP)

i) Queen Victoria School, Dunblane

j) St Benedicts Catholic School, Suffolk

k) Wallace High School, Stirling

## Summary of responses: proposals to tackle online abuse

The major activity in the Committee's session asked young people to evaluate possible ways to resolve or address online abuse. Students were asked to rotate around various proposals and assess them for their advantages and disadvantages.

Students evaluated the following proposals:

- Require ID to set up a social media account
- Ban anonymous social media accounts
- Limit who can comment on posts
- Run anti-prejudice public awareness campaigns
- Automated removal of posts containing rude and offensive words
- More education in schools about how to behave online

In some schools, students voted on the proposals as if they were members of the Petitions Committee deciding on recommendations for the Government:

- At De Warenne Academy, Yorkshire, students voted against all proposals except those to increase education in schools and to run public awareness campaigns.
- Students followed the same pattern at Wallace High School in Stirling: a minority voted in favour of proposals to require ID, remove or limit posts, and ban anonymous accounts. The majority voted in favour of anti-prejudice campaigns and increasing education in schools.

### *Require ID to set up a social media account*

#### *Pros*

In their responses, students identified that a positive effect of requiring ID for social media accounts would be that social media companies and other bodies would find it easier to track down perpetrators of online abuse.

They identified that a requirement for ID might make the online world safer for children, both in reducing the likelihood of "catfishing" and preventing underage children from having accounts. For example, some said that:

- "[A requirement for ID] Would prevent people managing to set up fake accounts"
- "[ID] Would result in "less catfishing"
- "[ID would] Stop underage kids from seeing bad things"
- "[ID would] Protect children against older potential predators"

Some noted that, compared to other potential methods, a requirement for ID represents a more permanent solution to stopping online abuse. They said that:

- It would "make sure that people can't keep setting up new accounts"
- "Banned people are always banned"
- "This actually requires and forces something"

They saw a requirement for ID as having a preventative effect:

- "As people are more likely to be identified they may not want to put nasty things"
- "It stops anonymous abuse"

### *Cons*

Across all schools that fed back to the Committee, young people identified a series of problems with the suggestion to mandate ID for social media accounts.

Many young people expressed distrust in sharing this level of personal data with social media companies. For example, they said that:

- [Social media companies can] "Easily take your personal information"
- "I don't want social media companies to have access to our IDs. This is a privacy issue, and they already have too much information."
- "Facebook is already stealing data–I don't want to share more".

They identified that it would increase the risk of data theft from outsider users. For example, they said that:

- "My data could get hacked"
- "This would really increase the risk of identity theft"

Young people told the Committee that, even with a requirement for ID, people would manipulate the system.

- "With this, there are ways to bypass it. People could use a fake ID. People can lie, use false info".

They were concerned that a process to provide ID would be bureaucratic and would "take a lot of time consuming to verify".

The most common disadvantage that young people identified was the barrier that a requirement for ID would create for users. They were concerned at the impact of this requirement on young people, many of whom said they do not have access to ID and said they won't need ID until they're 17 or 18.

Some students identified a risk for young people whose parents manage their ID. They said that there are some reasons that young people might want to use social media in secret. A group of students gave the example of someone who is LGBT+ and who'd like to access online support but for whom it's not safe to be "out" at home. Students said it might put these people at risk to ask their parent for their ID.

Several students identified that a requirement for ID "would disadvantage certain socioeconomic groups because of how much it costs to get ID".

### *Ban anonymous social media accounts*

#### *Pros*

Young people identified that a ban on anonymous accounts would increase accountability on the internet. They said that this would prevent trolling and bullying. They said that:

- This would "Massively prevent the safety net behind trollers/ racists"
- "Accounts purely for abuse are prevented"
- "Stops people from being unidentified, which would have a positive impact on their comments as they would be less likely to say cruel things."
- "Ensures people can't impersonate others or hide identity for purposes of abuse"
- "Stops stalking"

#### *Cons*

The most common concern expressed by young people was the effect of this proposal on privacy. Young people identified that there are different groups which might want to be anonymous online. This included:

- Young people: "Little children sometimes need to hide their accounts from older people"; "Anonymous accounts are safer for young people so that parents feel happier about them having accounts on social media"
- Fan accounts
- People involved in political campaigning
- People wanting to "interact with friends far away" without wanting close friends or family to see
- People at risk: "NO. People like to stay private e.g. on Twitch or Discord. Fake names to protect their information from potential trackers."

More broadly, students were concerned about their rights to privacy. There were many comments relating to this, including:

- "[A ban on anonymity] infringes my privacy rights"
- "[It would] Stop freedom of speech"
- "[It] restricts freedom"
- "People should be free to use the internet without having to disclose personal information"

- "Anonymous accounts aren't always wrong. Some people just don't want their lives public."

Some young people commented that this doesn't fit with people's preference for using sites seamlessly without logging in:

- "Sometimes I don't want to sign up or log into an account so I stay anonymous (I'm not really bothered to log in or I don't know why I should)"

Others stated that anonymity would be "hard to define":

- "Accounts may appear anonymous to older people but may be people that we know in the real world and are recognised as that online."

### *Limit who can comment on posts*

#### *Pros*

Students identified that a broad benefit of limiting comments would be that this would "reduce the likelihood of negative comments". They said that:

- "This might mean no more cyber bullying. No more hate comments".
- "[It] Would give people choice about who can comment and would reduce the online abuse as they could choose their friends and family to comment only."

They said that it would strengthen users' ability to block negative comments: "You will easily know who to report and get banned". One student said that this would "reduce anxiety of negative comments and reactions to posts".

One student identified a secondary effect that this might "limit grooming".

#### *Cons*

Students in several schools commented that this function already exists on some apps, for example "you can already 'switch off' and 'limit comments' on Instagram". This caused some criticism of the effect of limiting comments. Some students felt that it already wasn't working to reduce online abuse: one student wrote "it's already in place and isn't doing much–people find other ways".

Students identified the difficulties of limiting comments …

- "People could easily get to your post fast enough to comment"
- "Could be discrimination in who can comment"
- "There could still be people who can comment who would comment nasty things"
- "You don't know if people are being sarcastic"

… and that a limit on who comments might reduce accountability from users:

- "People won't be held accountable"
- "Wouldn't allow people to call someone out on posting something inappropriate"

As with the proposal to ban anonymous accounts and the proposal to require ID for users, students in most schools expressed concern that a general limit on who comments on posts would affect their freedom of speech. They said that it might also reduce the diversity of views online. They said that:

- "Limiting my comments means that I can't express opinions"
- "Echo chambers might become even more problematic."
- "You can maybe wanting to say a nice thing."
- "Restricts freedom of speech online, vast majority of people WILL NOT post offensive material"

Some students identified that this might cut off connection between users online:

- "People may want to get to know you and may not know you personally"
- "Someone might want to compliment you but not know you"
- "Reduce positive feedback or constructive criticism"

Some students commented on the impact of this proposal on their user experience. This applied to them as individual users:

- It "can be really annoying to not be able to comment on posts"
- "If the only people who comment are family it may be embarrassing"

And they said that it applied to people using social media for business purposes:

- "[This] Would not be useful for influencers, who may need the feedback."
- "This would be bad for celebrities, influencers, online shops. If it is mandatory."
- "Wouldn't work for business accounts"

### *Automated removal of posts containing rude and offensive words*

#### *Pros*

Students identified that a general advantage of posts being automatically removed would be a reduction in offensive comments online. They said that "fewer hate comments equal more positive vibes".

Some students found that, as opposed to manually limiting comments on posts, an automated system might solve problems more quickly:

- "Bad comments get taken off quicker"
- "Comments are removed to stop them from ever being seen"

- "Could stop mean things forever because they would be banned"

They identified that this would reduce the workload on moderators and might be "low in cost" compared to other approaches.

### *Cons*

Students' most commented criticism of this proposal was their view that artificial intelligence cannot judge the nuance of language online. Many students were concerned that an automated system would lead to the removal of the "wrong comments". They said that:

- "Bots might remove nice comments"
- "People who are sticking up for people could get taken down too"
- "Friends who are joking may get banned"
- "How would this identify new words? (invented could be worse)"

Students said that users could easily circumvent the system, for example by "wording out comments differently" or "you could just lie about who said it".

Again, young people were concerned about the implications of such a proposal on their freedom of speech:

- "No freedom of speech"
- "People can't express their feelings"
- "Based off opinion and morality–what someone may find offensive, someone else may not "
- "Internet would be censored completely"

As with the proposal to limit comments on posts, some young people felt that this would reduce accountability online: "With the automated removal, people will not be able to learn from their mistakes" and "There would be no real sense of punishment".

Some students gave examples where social media companies had attempted to block certain offensive words but had inadvertently blocked positive initiatives. One student gave an example of accounts campaigning for LGBT+ pride being blocked on TikTok which misjudged that they were homophobic. This student said that these cases undermine social media companies in their efforts to combat online abuse and that this results in people taking companies less seriously.

### *Run anti-prejudice public awareness campaigns*

#### *Pros*

Students generally identified that an anti-prejudice awareness campaign might make people who face abuse feel seen, and might cause people to consider others before posting something that could be abusive. For example, they said that a public awareness campaign might mean that:

- "People can feel safe being themselves"
- "Trolls could be helped to think before they speak"
- "The message gets to the community"
- "Kindness is enforced online"
- "People who may have not realised are made to care"
- "There is more emotional connection with people who may face bullying online"

#### *Cons*

In all schools where students fed back to the Committee, students commented that it was likely that public awareness campaigns would be ignored. Their critique of the proposal was wide-ranging. Many simply felt that people don't change their views after being exposed to a campaign:

- "There are better solutions and I personally think that people won't change their behaviour anyways."
- "Biggest issue of a public awareness campaign is not everyone sees it"
- "They're easily forgotten"
- "Campaigns don't often work"
- "No one will listen realistically"
- "More effort than what they will get back"
- "They encourage slacktivism"
- "Do campaigns have a long lasting effect?"
- "Pointless because even if people have been affected by online abuse they will be too scared to speak up and join in."

Some students were specifically concerned that a campaign with a strong message would entrench the views of people who oppose the message:

- "They can produce a defensive response which defeats the purpose and creates further division"

- "They might fuel pro prejudice campaigns"
- "Won't change views of racist people"
- "May be overshadowed by others' beliefs and views so the point is lost."

Many students expressed concern at the potential cost for the Government of running a major anti-prejudice campaign.

### *More education in schools about how to behave online*

#### *Pros*

Unlike a general public awareness campaign, some students felt that education from their own teachers might be effective in tackling online abuse. They identified that teachers can help students to "feel safe to be themselves", to "Draw clear boundaries of what is acceptable and not acceptable" and to show students how to build "A more civilized online world".

Students had specific ideas on what improved education in schools could look like:

- "Teach us how to report and block others. And what to report."
- "I think you should teach some younger people to not trust people online. You can't trust strangers."
- "I feel that we should have more anti-bullying staff in school and more anti-bullying lessons."
- "I feel like we need to educate children from around the age of 11–12 about the dangers of social media and how to behave correctly online. People who are repeatedly misbehaving online should have their accounts banned. Should teach lads not to share personal information online."
- "I feel like we need to educate people on racism and homophobia online."

Many students used the session to call for more education at a younger age. They said that they felt that when it was included in the curriculum they had already been online for a number of years.

#### *Cons*

As with the proposal for public awareness campaigns, students identified that increased education in schools might still be ineffective in changing people's minds. Some students were concerned that people would simply find other ways to bully: "Might encourage people to get the wrong idea and do it physically instead of online", "People might learn to disguise bullying better".

Some students said that messaging from older generations might come across as outdated:

- "Advice from teachers is outdated, not what young people listen to."

- "They won't understand. Abuse only affects people in school, not older generations."

This led some students to conclude that any education about online abuse should be led by their peers: "Younger people should teach as the teachers do not have the same experiences of online abuse so cannot relate".

Other students thought that the need for more education was not the responsibility of schools:

- "This is not the school's responsibility, should also be the Government and social media platform"
- "Behaviour online should be taught by parents"

Some students were concerned that dedicating time to teaching about online abuse would reduce their learning in other subjects and might affect their performance in exams.

## Other solutions

As well as considering the proposals from the Committee, students came up with their own solutions that the Government and social media companies could adopt to tackle online abuse. These included:

- "If someone has been found guilty of committing online abuse, social media companies should ban their whole device. This would prevent the person from using the same device to open another account"
- "Social media companies should look into something that's being reported and have three strikes and then have their accounts blocked"
- "A solution could be that social media companies warn you before you post something that AI thinks might be offensive"
- "People who aren't your friends on social media shouldn't be able to add you to group chats"
- "People should be able to have two attempts at having an account on each platform, max"
- "Students should have a school ID card which enables them to join social media for secondary school students."
- "The Government should survey people first it wants to blacklist certain words"
- "Social media companies could filter content only allowing people over certain ages to see some content. You could have your parents and guardians confirm your age so it is most likely correct and parents and guardians will be aware of their children having social media. Email can be used to confirm parents and guardians identity."

- "Instead of automated removal of posts, have a filter system for offensive and rude comments/ words. This needs to be a manual system to check to see context. Posts need to be able to be appealed."

## Other comments

Students were invited to share final thoughts at the end of the session. Some students were prompted to record what they thought was the most important thing to tackle. Other students were given a more open prompt to record what's most important to them about a safer online world.

In both this activity, and the other activities in the session, one of the common concerns among young people was the prevalence of racism on social media. In every school that fed back to the Committee, at least one student responded that racism was their biggest concern. Many students commented that racism isn't treated seriously enough by companies:

- "I think that serious comments such as death threats and racism should be treated harsher."
- "People don't care about racism. Should be police involved."
- "Gender discrimination is more cared about than racism."

In some schools, students were asked if they reported abuse when they saw it online. Many students said they had experience of reporting abuse online. Some students recorded a positive experience of reporting; across several schools, PlayStation was commented on as being particularly proactive when the students reported abuse. However, the majority of students in both their written comments and verbal responses during the sessions said that they felt that reporting abuse rarely led to anything. Many students didn't know what happened when they reported abuse. Some students said that:

- "As a group we're very concerned that when we report a post we never find out what the consequence was. We would like to be followed up with to know if the social media company has taken our claim seriously or not."
- "Social media companies should actually check reports (there are lots of reports that has nothing done about them)"
- "Does someone actually watch over the video which has been reported?"
- "Sometimes report buttons don't work and you feel as though you did something about it but you haven't"
- "I think [social media companies] could take quicker action to the bullying online because there are kids that get threatened every day and report it but still nothing is done so they should be checking comments daily"
- "I think social media companies should make the report / block button easier to find. More of a variety of ways to report someone for their actions."

# Formal minutes

## Tuesday 25 January 2022

## Members present

Catherine McKinnell, in the Chair

Elliot Colburn

Martyn Day

Matt Vickers

## Tackling online abuse

Draft Report (*Tackling online abuse*) proposed by the Chair, brought up and read.

*Ordered*, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 113 agreed to.

Annex agreed to.

Summary agreed to.

*Resolved*, That the Report be the Second Report of the Committee to the House.

*Ordered*, That the Chair make the Report to the House.

*Ordered*, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order 134.

## Adjournment

[Adjourned till Tuesday 1 February at 2pm

# Witnesses

The following witnesses gave evidence. Transcripts can be viewed on the inquiry publications page of the Committee's website.

### Thursday 21 May 2020

**Bobby Norris,** petition creator — Q1–13

### Thursday 2 July 2020

**Katie Price,** petition creator; **Amy Price** — Q14–60

### Tuesday 2 November 2021

**Nancy Kelley**, Chief Executive, Stonewall; **Danny Stone MBE**, Chief Executive, Antisemitism Policy Trust; **Matthew Harrison**, Public Affairs and Parliamentary Manager, The Royal Mencap Society — Q1–22

**Ruth Smeeth**, Chief Executive, Index on Censorship; **Chara Bakalis**, Principal Lecturer, Oxford Brookes University; **Dr Joe Mulhall**, Head of Research, HOPE not hate — Q23–40

### Tuesday 16 November 2021

**Seyi Akiwowo**, Founder and CEO, Glitch; **Andy Burrows**, Head of Child Safety Online Policy, NSPCC; **Stephen Kinsella OBE**, Founder, Clean up the Internet — Q41–57

**Ellen Judson**, Senior Researcher, Demos; **William Perrin OBE**, Trustee, Carnegie Trust UK; **Dr Bertie Vidgen**, Research Fellow, The Alan Turing Institute — Q58–76

### Tuesday 23 November 2021

**Dr Nicholas Hoggard**, Lawyer, Law Commission; **Professor Penney Lewis**, Commissioner, Law Commission — Q77–93

**Katy Minshall**, Head of UK Public Policy, Twitter; **Rebecca Stimson**, UK Head of Public Policy, Meta; **Theo Bertram**, Director of Government Relations and Public Policy for Europe, TikTok — Q94–130

### Wednesday 1 December 2021

**Chris Philp MP**, Minister for Tech and Digital Economy, Department for Digital, Culture, Media and Sport; **Orla MacRae**, Deputy Director for Online Harms Regulation, Department for Digital, Culture, Media and Sport — Q131–164

# Published written evidence

The following written evidence was received and can be viewed on the inquiry publications page of the Committee's website.

TOA numbers are generated by the evidence processing system and so may not be complete.

1 Antisemitism Policy Trust (TOA0008)

2 Carnegie UK Trust (TOA0016)

3 Epilepsy Society (TOA0020)

4 Inclusion London (TOA0013)

5 Mencap (TOA0015)

6 NSPCC (TOA0019)

7 Protection Approaches (TOA0018)

8 Twitter (TOA0012)

9 UK Interactive Entertainment (TOA0014)

10 Women's Aid Federation of England (TOA0011)

11 KIND ONLINE (TOA0010)

# List of Reports from the Committee during the current Parliament

All publications from the Committee are available on the publications page of the Committee's website.

## Session 2021–22

| Number | Title | Reference |
|---|---|---|
| 1st | Impact of Covid-19 on new parents: one year on | HC 479 |

## Session 2019–21

| Number | Title | Reference |
|---|---|---|
| 1st | The impact of Covid-19 on maternity and parental leave | HC 526 |
| 2nd | The impact of Covid-19 on university students | HC 527 |
| 1st Special | Fireworks: Government Response to the Committee's First Report of Session 2019 | HC 242 |
| 2nd Special | The impact of COVID-19 on maternity and parental leave: Government Response to the Committee's First Report | HC 770 |
| 3rd Special | The impact of Covid-19 on university students: Government Response to the Committee's Second Report | HC 780 |