House of Commons

Petitions Committee

Tackling Online Abuse: Government Response to the Committee's Second Report

Second Special Report of Session 2021–22

Ordered by the House of Commons to be printed 22 March 2022

HC 1224
Published on 28 March 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*)

Marsha De Cordova MP *(Labour, Battersea)*

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)*

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), Ed Faulkner (Second Clerk), Stella-Maria Gabriel (Committee Operations Manager), Hannah Olbison (Media Relations Manager), 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

Second Special Report

On 1 February 2022, the Petitions Commitee published its Second Report of Session 2021–22, *Tackling online abuse* (HC 766). On 17 March 2022 we received the Government Response to the Report, which is appended below.

Our conclusions and recommendations are in **bold**, followed by the Government's response to those conclusions and recommendations.

Government Response

Executive Summary

The government is grateful for the Petitions Committee's work in scrutinising the draft Online Safety Bill. The government agrees that online abuse can have a devastating impact on those who are exposed to it. The Online Safety Bill is an ambitious piece of legislation that will transform the experience of users online and usher in a new era of accountability for the tech sector.

The government is clear that online abuse is unacceptable and online platforms should never be a refuge for abusive, harmful or criminal behaviour. The Bill will ensure that illegal abuse is handled swiftly and effectively. Sites in scope of the Bill which are likely to be accessed by children will need to protect them from abusive content that does not meet the criminal threshold. The Bill will also ensure that high risk and high reach services, known as Category 1, will need to address certain types of online abuse content in their terms of service for adult users.

The new regulatory framework enshrines safeguards for users' rights online. It is vital that adult users are able to engage in robust debate online without fear of arbitrary censorship by tech platforms. At the moment, too many users feel unable to express themselves online because of fear of threats or harassment. The legislation is also tightly focused on services which pose the greatest risk of harm to users and where there is currently limited regulatory oversight.

In addition, the government is ensuring the criminal law is fit for purpose and able to hold individuals to account for their harmful communications online. The government asked the Law Commission to review existing criminal law for harmful communications online and offline. Following the Law Commission's final report, the government confirmed that it is accepting the harm-based communications, false communications and threatening communications offences which will be brought into law through the Online Safety Bill. We will also take forward the proposed cyberflashing offence through the Bill.

Alongside making legislative changes through the Bill, the government is committed to supporting the empowerment of users with the skills and knowledge they need to make safe and informed choices online. In July 2021, the government published the Online Media Literacy Strategy which introduced the Media Literacy Framework and sets out the key skills and knowledge underpinning strong media literacy capabilities. This promotes skills such as critical thinking and understanding that online actions have offline consequences. Alongside the Strategy we published the first annual Online Media Literacy

Action Plan. This includes funding media literacy organisations to support teachers and schools working with students with disabilities, upskilling library staff and youth workers and establishing an expert Media Literacy Taskforce.

Protecting UK users online is at the heart of the Online Safety Bill and the government's wider work. The government has welcomed the wealth of stakeholder expertise and lived experience. Survivors of online abuse and expert organisations have contributed to the development of policy and strengthening of the Bill's provisions. This report by the Petitions Committee is welcomed by the government and our responses to the Committee's recommendations are set out below.

The experience of people receiving online abuse

Recommendation 1: 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)

Government response

We thank the Committee for this recommendation. The Online Safety Bill will require the largest service providers to publish annual transparency reports. The Bill sets out a high level list of information that Ofcom can require services to report on. These reports will set out information about the steps these services are taking to tackle harms on their platforms. This includes information about the incidence of illegal and harmful content, information about the processes in place for users to report illegal and harmful content, as well as information on the measures being taken by a service provider to provide for a higher standard of protection for children than for adults. These reports will help Ofcom and users understand the prevalence of online harms and may provide insights into the level of violence against women and girls content online.

Ofcom will also produce an annual transparency report which will include information about the contents of the reports services have published. Furthermore, Ofcom will have the power to require services to provide information directly to Ofcom, including to support its research activity, which could also provide insights into violence against women and girls online.

Separately Ofcom will carry out risk assessments, covering illegal content, content that is harmful to children and legal content that may harm adults to identify, assess and understand the risks of harm to individuals presented by services. It will publish a register of risks, reflecting the findings of the risk assessments.

Ofcom will also carry out regular reviews looking at the incidence and severity of content that is harmful to children and content that is harmful to adults on services. Ofcom will publish a report after each review which will include advice on whether to make changes to priority harms to children and adults.

The Online Safety Bill

Recommendation 2: 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)

Government response

We agree that it is important to be clear and comprehensive about what types of content are harmful to children and to adults, but are taking a different approach to that suggested by the Committee. It is essential that the regulatory framework is evidence-based, flexible and future-proofed. The Online Safety Bill will create a framework under which the government will consult with Ofcom before designating categories of priority harmful content in secondary legislation. Service providers will have duties to protect children and adults from this designated priority content.

As well as creating the legislative framework for designating priority harms, the Bill will include clear definitions of non-designated content that is harmful to children and will set out the priority content that is harmful to adults. Service providers will have additional duties to protect children from this non-designated harmful content, and must report to Ofcom on any non-designated content harmful to adults that they become aware of.

Designating priority harms in secondary legislation will mean that they can be kept under review and updated to reflect emerging harms without requiring any changes to primary legislation. This will also allow for parliamentary oversight and democratic debate about the harms to be included in the list. This approach balances the need to give certainty to businesses on the harms they must address, whilst ensuring the legislation remains agile and flexible to emerging harms.

Recommendation 3: 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)

Government response

We thank the Committee for this recommendation. The government has taken a consultative approach throughout the Bill's development. The Bill is clear on what the Secretary of State's review of the regulatory framework must consider. In carrying out the review, the Secretary of State must consult Ofcom, and others as the Secretary of State considers appropriate. This provides the Secretary of State with the flexibility to consult those who may have useful views so that these can be taken into account in the review.

More generally the Bill provides for extensive consultation by Ofcom of organisations representing children and users. In particular, Ofcom will be required to consult with organisations that represent the interests of children and of those who have suffered harm as a result of online content when developing its codes of practice. It will also be required to conduct research into users' experiences of regulated services, which will enable Ofcom to better understand the needs of children and other affected users.

Ofcom has existing duties under section 16 of the Communications Act to consult with consumers about carrying out its functions and to establish and maintain the Communications Consumer Panel to advise Ofcom about matters relating to the internet of consumers of regulated services. These duties will be extended to services regulated under the Bill. Ofcom may also use other mechanisms to understand users' attitudes and concerns, such as research or activity undertaken as part of Ofcom's media literacy duties. This range of powers which will ensure Ofcom has all the tools it needs for understanding users' concerns and experiences.

Given these provisions in the draft Bill we do not think it is necessary to establish a statutory duty for the Secretary of State to consult civil society organisations or other groups in relation to the Secretary of State's review or more generally.

Recommendation 4: 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)

Government response

We agree with the Committee's suggestion that hate crime offences and offences associated with Violence against Women and Girls should be listed as priority illegal offences on the face of the Bill. Government announced this change on 5 February. This includes offences relating to sexual images (i.e revenge and extreme pornography), and harassment and stalking offences, as well as acts intended to stir up racial hatred, religious hatred or hatred on the grounds of sexual orientation and racially or religiously aggravated harrassment and public order offences. This means all services will need to take steps to remove, and prevent users from being exposed to this content. This will result in women and girls being better protected online and proactive measures to tackle illegal abuse on the grounds of the listed characteristics.

Beyond the priority offences, all services will need to ensure that they have proportionate systems and processes in place to quickly take down other illegal content directed at women and girls once it has been reported or they become aware of its presence.

Recommendation 5: 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)

Government response

We agree that companies should be required to give separate consideration to the risks faced by different user groups. We have therefore amended the risk assessment provisions to require companies to consider the risk of harm to individuals with a certain characteristic or due to membership of a certain group. This includes, but is not limited to, the protected characteristics.

Recommendation 6: 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)

Government response

We thank the Committee for this recommendation. The Online Safety Bill is designed to bring into scope services which pose the greatest risk of harm to users and where there is currently limited regulatory oversight. In order for the regulatory framework to be effective, the scope of the Bill must be targeted and proportionate.

This legislation is intended to protect children not only on services which are targeted at them, but on any in-scope services which they are likely to access. All services will need to assess whether their service is likely to be accessed by children and if so, deliver additional protections for them. The child user condition is met if children form a significant number or proportion of users on a service, or if the service, or any part of it, is of a kind that is likely to attract a significant number or proportion of child users. This condition has no relation to a platform's size; a service will meet the condition if a significant number or proportion of their users are children.

Services who do not consider they are likely to be accessed by children will need to record the evidence that they have that children are not accessing their service, and keep this under review. The requirement to undertake, and keep up to date, a suitable and sufficient assessment about child access is an enforceable requirement. Ofcom may take enforcement action where providers do not carry out an assessment and keep it up to date, (and might be alerted to this via user complaints for example), including the potential for fines.

Recommendation 7: 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)

Government response

We thank the Committee for this recommendation. An overarching principle of the Bill is to ensure that what is unacceptable offline is also unacceptable online. This is why all in-scope services will be required to tackle illegal content and ensure any children using their services are protected from harm.

Recognising the influence of larger platforms, the Bill also introduces a categorisation approach to ensure the most used services are accountable to their users. Services providing high-risk, high-reach services (known as Category 1 services) will therefore have a legal obligation with regard to content and activity which is legal for adults but may be harmful to them.

However, we do not think it is appropriate for the Government to require platforms to remove or interfere with legal content. This is why the duties are focused on increasing transparency about the risks on Category 1 Service, and ensuring companies set and enforce clear terms of service for how they will treat harmful content. This will enable users to make informed decisions about the platforms they use.

This approach is also designed to be proportionate and to not place burdens on smaller services that do not have high reach, recognising that adult users may wish to seek out this content. Moreover, harmful material is likely to cause the most harm on Category 1 services with the largest audiences and a range of high-risk features, where it can spread quickly and reach large numbers of people.

Recommendation 8: 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)

Government response

We thank the Committee for its suggestion. However, we do not believe that reformulating this regulatory framework around a single foundational duty would be desirable or effective. It would leave Ofcom with very high-level duties to enforce against which would likely create an uncertain and unclear operating environment. Such an environment could also lead to a reduction in legal certainty for services, Ofcom and users as well as potential delays to the vital safety benefits for users that this legislation will bring.

The framework will improve user safety by creating duties on platforms to assess risk for specific categories of harms, and to put in place systems and processes to mitigate identified risks. The Bill directly requires service providers to assess the risk of harm linked to how their services are designed and to consider how a comprehensive range of functionalities and the way in which people use their services affect risk. For example they will have to look at how users can send messages to or play games with other users and express views on content through "likes" or voting.

The duties include specific requirements to put in place proportionate systems to remove and limit the spread of illegal content and to protect children from harmful content. The largest services will also need to set and enforce clear terms of service for tackling legal but harmful content.

Online Abuse and the Criminal Law

Recommendation 9: 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)

Government response

We welcome the Committee's recommendations regarding the Law Commission's review, 'Modernising the Communications Offences.' The government's interim response to the Law Commission's review confirmed that the Bill will incorporate the Law Commission's recommended harmful communications offence, threatening communications offence, false communications offence. The Bill will also include the Law Commission's recommended cyberflashing offence.

We note the Committee's comments related to the interpretation of the harm-based offence. The offence—and the other new communication offences—will ensure that the criminal law is focused on the most harmful behaviour while protecting free expression. The government also anticipates the Crown Prosecution Service's (CPS) will update the guidelines on prosecuting cases involving communications sent via social media. We will monitor the implementation of the new communications offences and its impact on the criminal justice system once these offences come into force. Notifiable offences are collected from police forces on a monthly basis and published within the quarterly Crime statistics by ONS found here Crime in England and Wales—Office for National Statistics (ons.gov.uk).

Recommendation 10: 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)

Recommendation 11: 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)

Government response to recommendations 10 and 11

We thank the Committee for its recommendation to scale up existing specialist teams and to ensure police officers are able to access the right training to identify offences and support victims of hate crime. We are carefully considering the recommendations set out in the Law Commission's final report, 'Hate Crime Laws,' and will shortly publish a new strategy for tackling hate crime, setting out our commitment to stamping out these abhorrent crimes including their online elements, which cause greater harms to victims and associated neighbourhoods.

Anonymity and accountability

Recommendation 12: 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)

Government response

The government agrees with this recommendation. The Online Safety Bill requires service providers in scope to identify, mitigate and effectively manage the risks associated with online anonymity on user-to-user services. As part of their risk assessments, all services will need to assess the functionality of anonymous and pseudonymous profiles and the role they play in allowing illegal and (for Category 1 services and services which are likely to be accessed by children) legal but harmful content to spread, and to implement appropriate protections.

Recommendation 13: 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)

Government response

We thank the Committee for this recommendation and will continue to keep it under consideration. The Online Safety Bill will require companies that are likely to be accessed by children to assess the risks to children from harmful content and activity on their service, including anonymous abuse, and provide safety measures. Category 1 services will also be required to identify, mitigate and effectively manage the risks associated with online anonymity which does not cross the criminal threshold, where this affects adults.

In its codes of practice, Ofcom will also set out the steps services can take to mitigate risks to users' safety from harmful content, including those arising from anonymous profiles. This could include steps services could take to ensure the appropriate use of identity verification before lifting bans on suspicious accounts and taking action against repeat offenders.

Where services do not comply with their duties, Ofcom can take robust enforcement action, including imposing substantial fines.

Recommendation 14: 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)

Government response

All online abuse is unacceptable and will be significantly reduced by the introduction of the online safety framework, regardless of whether it is anonymous. The government has engaged with law enforcement to ensure the current powers they have are sufficient to tackle illegal anonymous abuse online. The outcome of that work will inform the government's position in relation to illegal anonymous abuse online and the online safety regulatory framework. Decisions about the allocation of Police resources and deployment of officers are for Chief Constables and Police and Crime Commissioners. The Home Office continue to fund specialist investigation teams such as the Police Online Hate Crime Hub, the Social Media Hub and the Counter Terrorism Internet Referral Unit.

Recommendation 15: 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)

Government response

The government welcomes this recommendation and agrees that it is important that users are given the choice over who they interact with. The government has included new duties in the Bill on Category 1 service providers to give adult users more control over their online experience.

The new user verification duty will ensure that Category 1 service providers provide all adult users with the option to verify their identity, should they wish to do so. The recommended forms of identification by which users can verify their identity will be set out through guidance issued by Ofcom. As part of preparing the guidance Ofcom must ensure that the recommended verification measures are accessible to vulnerable users. In preparing the guidance Ofcom must also consult the Information Commissioner, persons with technical expertise, persons representing vulnerable adult users and anyone else they consider appropriate.

Alongside the user verification duty sits the new user empowerment duty. The user empowerment duty will ensure that Category 1 service providers provide adult users with the tools to control whether they encounter or interact with unverified users. This includes preventing unverified users from seeing their content or seeing content from an unverified user. In addition, Category 1 service providers, for harmful content that Category 1 services do tolerate, will have to provide users with the tools to control what types of legal but harmful content they see. This could include, for example, content on the discussion of self-harm recovery which may be tolerated on a category one service but which a particular user may not want to see.

These two new duties, in combination, will help provide robust protections for adults, including vulnerable users. They will ensure that UK users have more control over who they interact with and what content they see.

Department for Digital, Culture, Media and Sport

March 2022