Meta

December 14th, 2022

Dame Angela Eagle and Sir Roger Gale
Chairs, Online Safety Bill (Recommited Clauses and Schedules) Committee
House of Commons
London SW1A 0AA

Dear Chairs,

Meta was grateful for the opportunity to provide evidence to the Online Safety Bill Committee earlier this year. Our oral and written evidence is available on the Parliamentary website.

You will be aware that Meta has long supported the intentions behind the Online Safety Bill, and are keen to support the Government and Parliament in making it as effective and workable as possible. We understand that the Online Safety (Recommited Clauses and Schedules) Bill Committee is not taking formal evidence on all of the proposed amendments that the new Government has announced. It is regrettable that the Bill will not go through a full consultation process in the Commons, and that the Committee will need to rely on evidence from different sessions to address all of the amendments that have been raised.

For example, Section 106 (2b) of the Bill was introduced as an amendment by the Home Office to force companies to develop or source technologies for the purpose of detecting certain kinds of content. This amendment was introduced after the original Public Bill Committee and will not face adequate scrutiny before the Bill progresses, despite legal experts stating that this is a far-reaching surveillance power with little oversight (further details below).

Nevertheless, we would like to take this opportunity to share our views on the Bill as amended, and to share our concerns about the potential unintended consequences of the way the Government has drafted the final text. Given the extreme pressures on your Committee's time, we have focused on what we see as the top priority issues for Parliament to consider before the Bill is passed. These issues include the treatment of private messaging services in the Bill and the introduction of poorly defined concepts and in some places contradictory requirements on regulated services.

We would be happy to discuss any additional questions that the Committee may have, or any particular points in our recommendations if helpful.

Kind regards
Richard Earley
UK Public Policy Manager, Meta

Introduction

Meta has long called for new rules to set high standards across the internet. Even though we already have strict policies against harmful content on our platforms, regulations are needed so that private companies aren't making so many important decisions alone.

We share the Government's aim of making the internet a safer place, and there is much we welcome in this Bill:

- It attempts to establish a systems-based framework, focused on outcomes
- It requires companies to assess the risks of users encountering harms on their services, and then take proportionate steps to address those risks
- It sets high standards for transparency from internet companies about their rules and their work to enforce them, backed up by independent audit from Ofcom

However, over the long process of developing this Bill, it has been drawn away from this outcome-based approach, and parts of it are now overly complex, ambiguous and contradictory, or risk undermining user privacy. This risks making the Bill less effective and less workable.

- It introduces a number of poorly defined concepts and places contradictory requirements on services to limit the spread of some types of speech while protecting others, without clarifying how to balance the inevitable tensions this produces.
- It tries to tackle too many different issues, making it overly complex, and in places causing it to diverge from the intended focus on systems and processes, not single posts.
- It does not contain sufficient protections for people's privacy, especially in messaging services, and creates considerable powers for Ministers to direct the regulator Ofcom and lacks appropriate judicial oversight for far-reaching powers.

While we have shared details about these concerns with previous Committees, we enclose here further information that Meta believes the Committee should bear in mind about potential unintended consequences of the current text of the Bill.

1. Private Messaging

Section of the Bill and/or Government amendment

Section in the Bill (as amended on Report)
Schedule 11
Section 82
Section 6
Section 104 (Tech notices)
Section 105

Government amendments
NC11 - Notices to deal with terrorism content or CSEA content (or both)
NC12 - Warning notices

Concerns

The original Online Harms White Paper correctly made an important distinction between public platforms and private messaging, recognising the differences between the two. The Pre Legislative Scrutiny Committee reflected this, for example encouraging the Government to clarify how an encrypted service can comply with the Bill. However, the final Bill has done away with that distinction and now some (but not all) forms of private messaging are to be grouped together with public platforms as 'user to user' services. This raises many questions about what will be considered reasonable and proportionate steps for a messaging business to take towards people's private conversations while also protecting individual privacy and tackling harms.

For example, if provisions intended for public platforms which require the use of automated technologies to look for both harmful content for children and illegal content are applied in private messaging, this could result in companies having to monitor every private message to guarantee compliance with the regime. This would also undermine the security of millions of users according to the consensus of cybersecurity experts, as encryption is one of the most important tools to promote safety and security online. The Bill therefore needs to make it explicitly clear what a tailored privacy and encryption respecting approach looks like when it comes to a duty of care for private messaging services.

The second problematic area of the Bill in relation to private messaging is the technology notices powers. The Online Safety Bill was intended to be future proof, tech agnostic and focus on systems and outcomes. The technology notices part of the Bill is at odds with this approach as it gives Ofcom the power to force companies to adopt 'accredited' technology in certain circumstances. What the trigger point is for exercising those powers is unclear, how a technology is 'accredited' is also unclear, and how duties to protect privacy and ensure safety will be balanced is unclear. Ofcom can either impose a technology on a company or direct that company's R&D investment to have them develop new tools in this space, as well as require companies to change or re-engineer their services to enable accredited tech to work. These highly intrusive powers have very little checks and balances associated with them, with leading legal experts like Matthew Ryder KC questioning their legality, proportionality, and compatibility with the common law and human rights legal framework. If the 'accredited' technologies are indeed the client-side scanning proposals funded by the Government's Safety Tech Challenge Fund, this will amount to state mandated "surveillance of the content of communications on a generalised and widespread basis".

Proposed change to the Bill

A. **Amendments to give equal weight to users' privacy and online security throughout the Bill** - Currently the Bill only requires Ofcom to give regard to privacy in the following form: "[if it represents a] breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service." The Bill should make clear that UK citizens and consumers have a right to privacy - putting this on an equal footing to the 'right to expression' that already exists in the Bill.

B. **Providing explicit support for E2EE and clarity that technology notices cannot be used to undermine E2EE.** This would have been achieved by an amendment proposed during the first report stage (153) to prevent technology notices from applying to private messaging services. If a similar amendment is not made, amendments should be made to the Bill providing robust procedural safeguards (e.g. judicial oversight;

right to refer issuance of notice back, right of appeal to the High Court) and substantive safeguards (e.g. overarching duty to protect user privacy and security) around the issuance of technology notices.

C. **Provide clarity that providers of private messaging services should undertake a risk assessment process that would not result in mitigations that amount to monitoring or moderating content**

D. **Private messaging services and encrypted services should be explicitly exempt from being designated Category 1.** Alternatively, the Bill should restore the distinction between public social media and private messaging (as was in previous drafts of the Bill), and Ofcom should be explicitly required to set out how a service's duties should apply in private messaging via a Code of Practice.

2. **Verification**

Section of the Bill and/or Government amendment

Section in the Bill (as amended on Report)
Section 14 – User empowerment duties
Section 57 – User identity verification

Concerns
The Bill requires the largest services to give all existing and future users an option to verify their identity, and then to 'filter out' content from unverified users. While platforms have a responsibility to tackle online abuse, there is a lack of evidence to support the claim of a direct link between online anonymity and harm. It is not clear what steps services would be asked to take in order to verify a user, nor how they would indicate whether a user is 'verified' or not. This proposal could raise challenging issues about equitable access to identity processes, despite the assertion that documentation need not be required, given the UK Electoral Commission have estimated that 3m people in the UK have no means of official ID.

Moreover, the connected provisions in the related 'User Empowerment' section to enable 'filtering out' content could lead to a two-tier internet. Those unable or unwilling to disclose their identity online could be shut out from public discussion, particularly those from underrepresented groups or young people, who have less access to identity documents. And as the provisions are only to apply in the UK, British internet users could be walled off from the benefits of the open internet. It is also not clear how technically feasible these proposals would be for many services.

We have worked extensively to understand what tools and user controls do have an impact on preventing harmful behaviour, and to build and provide those tools to users. These include comment controls; comment warnings; Direct Message controls; the ability to block and restrict accounts; and the ability to limit interactions from accounts that don't follow or only recently followed you.

Proposed change to the Bill
The concept of verification is ambiguous. It is not clear the steps we would be asked to take in order to verify a user, or if we would be asked to indicate whether a user is 'verified', and if

implemented the 'user empowerment' provisions could lead to British internet users being shut out of online discussions. We would therefore advocate a removal of these provisions from the text.

If the Government still proceeds with the provision to require large services to offer users the option to verify themselves, then the Government should remove the link between this provision and the 'User Empowerment' duties enabling users to 'filter out' non-verified users.

3. **Journalism**

Section of the Bill/ Government amendment

Section in the Bill (as amended on Report)
Section 16 – Duties to protect journalistic content

Government amendment
NC19 - Duties to protect news publisher content

Concerns

Journalist Exemption
The Bill gives particular protections to "journalistic content", but the definition of this term and the expectations on companies are left poorly defined, creating a risk this exemption could be misused or have unintended consequences.

We are concerned that the Government is putting obligations on private companies to make extremely complex and real time assessments about what constitutes journalistic content which could be impossible to implement consistently. We would also question whether it is appropriate for platforms to be defining what counts as journalistic content.

We are also concerned that these requirements may inadvertently give a level of protection to bad actors, which may expose users to an increased risk of harm. This is especially the case when it comes to content from users who assert that they are operating as citizen journalists. We have already seen instances where some users claim they are citizen journalists in an attempt to reduce the likelihood of Facebook (and other platforms) taking action against them or their content.

Must Carry Obligations
The Government amendment (NC19) requires platforms to keep news articles up even if under review by moderators and platforms must notify news publishers and offer a right of appeal before taking any action.

We recognise that news is a public good, and we made significant investments in journalism in the UK. However, through this amendment, we are concerned that the Government is putting obligations on private companies to make extremely complex and real time assessments about what constitutes news publisher content which could be impossible to implement. We would also question whether it is appropriate for platforms to be defining who is a news publisher.

We are concerned our fact checking programs, aimed at preventing the spread of harmful misinformation, could be prevented from being able to fact check potentially false, dangerous or misleading information and therefore our efforts to protect people on our platform would be seriously hampered.

We are concerned that this amendment will also be placed in direct tension with the other duties such as addressing legal content that is harmful to children or adults.

Moreover, these protections are likely to incentivise bad actors and harmful websites to seek to qualify as recognised news publishers in order to avoid having action taken against them or their content. (e.g. because they publish legal but harmful content).

This amendment could considerably hamper our fact-checking efforts on our platform and potentially expose users to harmful content. This may result in seriously harmful content that goes against the standards set by platforms themselves (such as footage of a terrorist attack) would be required to stay online during a potentially lengthy review process.

Proposed change to the Bill:
There should be a provision in the Bill that clearly defines “journalistic content” i.e. from a person who creates news-related material, or exercises editorial control over such material, for a recognised news publisher.

This additional clause for a ‘temporary must carry’ will hamper platforms’ efforts to tackle harmful content, rather than resulting in a safer internet. It should be removed.