STRENGTHENING PRIVACY IN THE ONLINE SAFETY BILL

JOINT CIVIL SOCIETY BRIEFING JUNE 2022

SUMMARY

Privacy and anonymity are essential protections to keep people safe online, and allow them to exercise their digital rights and freedoms. The Online Safety Bill overlooks this, and sees privacy and anonymity primarily as constraints on the pursuit of safety or as risks to be managed. This briefing sets out why the protection of privacy and anonymity in the Bill should be strengthened, if the Bill is to deliver on its promises to keep users safer online and protect freedom of expression. It sets out how this can be achieved through strengthening rights protections and reducing the incentives for platforms to meet their safety duties through the use of systems which fail to protect the privacy of their users.

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

BACKGROUND

Privacy and anonymity are essential protections in a rights-respecting regulatory regime

The Online Safety Bill will be a world-leading digital regulatory regime, and as such will set a precedent for other governments on what a 'liberal democratic vision' of the internet means. A regime which fails to protect users' ability to use the internet to communicate securely, express themselves without fear of reprisal, or to access information freely, risks being replicated and used to justify human rights abuses globally.

In the Declaration for the Future of the Internet, to which the UK is a signatory, signatories commit:

- 'To work together to maintain a high level of security, privacy protection, stability and resilience of the technical infrastructure of the Internet'
- To ensure that the internet is 'developed, governed, and deployed in an inclusive way so that unserved and underserved communities, particularly those coming online for the first time, can navigate it safely and with personal data privacy and protections in place'
- To ensure that 'individuals and businesses can trust the safety and the confidentiality of the digital technologies they use'

As it stands, the Online Safety Bill fails to meet these ambitions.

The Bill will require, or introduces the ability to require, platforms to take measures that have serious implications for privacy and anonymity - including increasing ID verification, age verification, requiring the use of technologies to engage in user profiling and behaviour identification, and content moderation on private channels. Coupled with vague and limited provisions around protecting privacy, this means that there is a high likelihood of serious violations of privacy. These will compound rather than challenge the dominant models of data surveillance that platforms are able to monetise for their own profit, and not in the interests of their users.

Privacy and anonymity are essential for online safety

Lack of privacy or anonymity puts people at risk: from exposed data and communications increasing their susceptibility to fraud and crime, to being identified and tracked by abusers, to being at risk of physical violence through

doxxing and stalking, to being targeted for persecution. Technological violations of privacy and anonymity create the conditions for violence and human rights abuses to be perpetrated - such as in China, where the persecution of and atrocities against the Uighur people are facilitated through systems of mass data collection and technological surveillance.

It is widely acknowledged that anonymity is an essential protection for particularly at-risk groups - such as women at risk of domestic violence; human rights defenders, investigative journalists, those combating extremism, and whistleblowers; and groups who are at risk of persecution, violence or discrimination based on aspects of their identity, including LGBT+ people, disabled people, and BIPOC people.

However, anonymity is not just an essential protection for those most at risk, but for all internet users: there is a basic expectation that users should be more in control of who accesses their personal information, and in what spaces they choose to identify themselves. People accessing support forums online share highly personal information and need to be able to do so safely; sex workers rely on being able to control their online identities to work safely; journalists need to be able to communicate with their sources in a safe and secure way.

And it is not sufficient to protect users for their privacy and anonymity to be preserved only from other users in public forums. Platforms collecting, storing, sharing and selling personal data about users and their communications facilitates the possibility for targeted violence and harm against individuals where that information is misused. But beyond this kind of misuse, it is the *regular operation* of these advertising-driven platforms in how they treat user data that facilitates political and democratic manipulation, financial exploitation and fraud, and the sharing of sensitive personal data about users, such as health or identity data, without consent. This is a problem which is only likely to get more difficult: with the further development of the metaverse, the ways in which our activity, behaviour, personal data and identity can be monitored and policed will become ever more complex, and the data that can be collected and shared ever more intrusive.

The financial success of current platform models *depends* on people being deprived of privacy and anonymity. Regulation should be seeking to challenge this status quo, not reentrench it. The very platform systems which the Online Safety Bill seeks to regulate in order to reduce user harm are systems which rely for their successful operation on users having inadequate privacy and anonymity protections.

Privacy and anonymity are essential for freedom of expression

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

"Laws, practices and policies that ban, restrict, or otherwise undermine encryption and anonymity – all in the name of public order or counter-terrorism – do significant, and I would say disproportionate, damage to the rights at the heart of my mandate." - David Kaye, then-UN Special Rapporteur on freedom of opinion and expression

People being able to access internet services anonymously, without having to prove their identity, is a crucial protection, particularly for more marginalised or vulnerable users. Measures which seek to reduce anonymity or privilege identity verification online risk creating a two-tier internet where people are deprived of full and equal access to and use of essential communication services based on who they are rather than based on their behaviour. As well as those who cannot safely identify themselves online, ID verification requirements can disproportionately impact the access to information of people who have limited access to ID. This includes financially excluded people, undocumented people or those whose legal identification does not accurately represent their name or identity, such as many in the trans community.

Protecting end-to-end encryption

The current narrative around end-to-end encryption presents encryption as an unqualified threat to the protection of children, and as such, the Online Safety Bill contains provisions through which OFCOM can require companies to use 'accredited technologies' for content moderation in private channels. This is very likely in practice to permit OFCOM to require platforms to use technologies that are incompatible with the use of end-to-end encryption or that compromise its integrity.

Presenting the protection of privacy as being in fundamental opposition to protecting children from abuse is a false dichotomy. Although the intention may be to only use these provisions to further the detection of CSAM, once the integrity of an encrypted channel is compromised (e.g. by the introduction of a 'backdoor'), the risks of users' information being accessed and shared by bad actors, repressive governments or corporations, is significantly increased and can pose serious dangers. Claiming that the encryption needs to be compromised in order to stop bad actors is a narrative that can easily be reproduced to justify illegitimate and repressive policing regimes.

This does not in any way limit the expectation that platforms take significant steps to protect children and tackle CSAM, but that they do so in a way which protects and promotes the rights of safety of all users, including children. Encryption and privacy online protect children and adults online, as the ICO has acknowledged, and as such should be protected.

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

"E2EE [end-to-end encryption] serves an important role both in safeguarding our privacy and online safety…It strengthens children's online safety by not allowing criminals and abusers to send them harmful content or access their pictures or location." - Stephen Bonner, ICO ED

AMENDMENT AREAS

RIGHTS

The existing duties in the Bill to protect rights are extremely vague and overly narrow: platforms need only have regard to the importance of protecting privacy and freedom of expression, with little priority or specificity given to how this will be achieved.

Schedule 4 should be amended so that the online safety objectives for regulated user-to-user services and regulated search services both include rights protections, such as including that:

a) a service should be designed and operated in such a way that the human rights, as defined in the Human Rights Act, European Convention on Human Rights and UN Convention on the Rights of the Child, of users and affected persons are protected

CLAUSE 19 AND 29

Duties about freedom of expression and privacy

This amendment should add:

- that all services have a duty when deciding on and implementing safety measures and policies, a duty to have regard to the importance of protecting users' access to information.

And the clause should be amended to:

- When deciding on, and implementing, safety measures and policies, a duty to have regard to the importance of protecting users' Article 8 rights

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

- The additional duties for Cat 1 Services should be amended to extend the impact assessment to cover users' human rights as set out in the ECHR, and not only freedom of expression and privacy

PRIVACY

CLAUSE 9

- Language around users being 'prevented' from accessing certain forms of content, should be amended to 'minimising' or 'mitigating' risk using proportional systems and processes, to avoid mandating the use of technical systems that will overmoderate or over-restrict users' access to information.

CLAUSE 83-84

The amendment should be that in the course of its duties, in carrying out risk assessments, serving information or enforcement notices, and developing Codes of Practice, OFCOM should be required to carry out a rights impact assessment on the systems and risks that they are assessing and the systems or technologies they are recommending.

This should also set out that all measures set out in Codes of Practice to verify age or identity or use proactive or accredited technology should meet minimum standards to protect privacy.

CLAUSE 103-109

Requirements to use proactive or accredited technologies should also be subject to periodic review, including requirements for OFCOM to engage in consultation with rights experts to ensure that any requirements continue to be proportionate and rights-respecting.

That OFCOM must particularly consider matters including 'the level of risk of the use of the specified technology resulting in a breach of any statutory provision or rule of law concerning privacy that is relevant to the use or operation of the service (including, but not limited to, any such provision or rule concerning the processing of personal data)' should be strengthened to require OFCOM to complete and publish a rights impact assessment on the impact on the right to privacy, as defined in the ECHR, in consultation with human rights experts of their requirement to use that technology.

CLAUSE 140-142

The provisions for supercomplaints should specify that platforms' failures to protect privacy or access to information are also a grounds to bring a supercomplaint, rather than only harm and freedom of expression being mentioned on the face of the Bill

The amendment should be that supercomplaints can be brought also on the grounds that service(s) are:

a) significantly adversely affecting the right to privacy within the law of users of the services or members of the public, or of a particular group of such users or members of the public; or
b) significantly adversely the access to information of users of the services or members of the public, or of a particular group of such users or members of the public

Clause 185(2)

The factors to be considered when determining whether content is communicated publicly or privately should be expanded - currently they are

- (a) the number of individuals in the United Kingdom who are able to access the content by means of the service;
- (b) any restrictions on who may access the content by means of the service (for example, a requirement for approval or permission from a user, or the provider, of the service);
- (c) the ease with which the content may be forwarded to or shared with users of the service other than those who originally encounter it.

This should be expanded to include a provision about the degree to which users have a reasonable expectation that they control who sees information that they share within that space: which should be established by OFCOM explicitly in consultation with users and experts.

The amendments on Rights and Privacy are also supported by

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

ANONYMITY

As currently drafted, the universality of the user identity verification duties risk:

- compromising user privacy and facilitating wider surveillance by entrenching and incentivising even greater systems for data collection, retention and data sharing by tech companies;
- excluding marginalised groups from participating in democratic discourse: for instance, a young LGBT+ person who needed to remain anonymous online would likely find themselves excluded from engaging with other accounts or even have protections for their safety and security revoked
- compounding the problems which they are designed to solve: for instance, someone who had verified their identity with a platform but was spreading disinformation or carrying out scams might be more trusted by other users by the perception they had been determined to be 'legitimate'
- failing to solve the problem of anonymous abuse by giving users control over the attributes of the people they interact with rather than the behaviour of who they interact with

We propose that:

CLAUSE 14; CLAUSE 57 and 58

The user identity verification duties and user empowerment duties be deleted from the Bill

Failing that: we suggest that

The amendment replaces the requirement for Category 1 services to offer users the option to verify their identities with the option to verify their personhood (through a method determined through a platforms' risk assessment to be most appropriate - e.g. by periodically confirming their personhood during the initial phase of the use of their account).

This would enable users to verify that they are human, without having to identify which human they are - tackling the risks associated with bot and inauthentic accounts, while decreasing the risks of privacy and exclusion of people for whom it is not safe or possible to link their identity to their online presence.

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

And to add:

'If a provider of a Category 1 service offers or requires adult users of the service to verify their identity, they must:

1) Do so in accordance with minimum standards for privacy protection, to be set out in guidance by OFCOM
2) Produce and publish a rights impact assessment setting out how rights, including privacy rights, the right to anonymity, freedom of expression and information access might be affected by the system they have in place, and what steps the platform is taking to mitigate these threats'
3) Do so in accordance with minimum standards for user service provision, set out by OFCOM, requiring that platforms do not take discriminatory action against unverified accounts beyond what the user empowerment duties require users to be able to choose'

These amendments on Anonymity are also supported by 

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk

Briefing prepared by Ellen Judson, CASM, Demos. For queries, please contact ellen.judson@demos.co.uk