Pointmaker

A CENSOR'S CHARTER?

The case against the Online Safety Bill

By Matthew Feeney

SUMMARY

- The Online Safety Bill (OSB) was introduced with noble intentions, to address genuine social harms taking place online.
- But the resulting legislation represents a grave threat to free speech, which will encourage online services to be excessively zealous in removing perfectly legal content from their platforms, in order to avoid multi-billion-pound fines.
- The OSB also threatens privacy. The Bill imposes obligations on online services that would weaken or remove encrypted communication services, as well as encouraging them to engage in greater surveillance of their platforms and in some cases to collect personal identifiable information from visitors.
- The OSB will entrench market incumbents, which are best-positioned to comply with the Bill.
- The OSB will hamper innovation and investment. The Bill covers far more than the social media industry, and will be a deterrent for investors and entrepreneurs across a wide range of technology sectors who are considering committing to investment in the UK.

INTRODUCTION

In 2018, Secretary of State for Digital, Culture, Media and Sport Matt Hancock introduced new legislation intended to make the United Kingdom the 'safest place in the world' to be online.[1] The next year, the Government published its Online Harms White Paper.[2] The paper outlined an ambitious set of policies targeting the spread of harmful online content such as child sexual exploitation and abuse, terrorism, hate speech, revenge pornography, extreme pornography, harassment, bullying, encouragement of self-harm and suicide, modern slavery and incitement to violence. These policies included obligations imposed on online services under a 'duties of care' scheme.

While the Government may be selling the Bill as a 'world-leading' piece of safety legislation, it is best understood as a significant threat to civil liberties, innovation and competition.

In 2020, CPS senior researcher Caroline Elsom published a paper describing the harmful, unintended consequences that would result under the Government's plans.[3] She correctly noted that the duties of care would hamper competition, encourage online services to restrict speech, stunt innovation and put the privacy of law-abiding British residents at risk. In particular, her work focused on the obvious injustice of policing speech differently online and offline; the scope for creeping censorship inherent in the fuzzy concept of speech that was 'legal but harmful'; and the lack of democratic accountability in delegating such judgments to Ofcom (the Office of Communications, a government regulator) rather than having them made in Parliament.

While defending the core principles of the Bill, the joint parliamentary committee chaired by Damian Collins MP – set up to improve legislation that was widely acknowledged to be deeply flawed – accepted the justice of the CPS's arguments in terms of the need to find a balance between censorship and public safety. He explicitly acknowledged our paper's influence in proposing that the relevant clause of the legislation be removed, to ensure that the list of offences both online and off was grounded in existing and proposed law.[4]

Unfortunately, Hancock's successor Nadine Dorries MP went in a different direction. She introduced the Online Safety Bill (OSB) in March 2022 without addressing the risks Elsom and many other policy experts identified.[5] She also took a different approach to online safety from Hancock, shifting much of the rhetoric away from an emphasis on safety (and an accompanying recognition of the economic significance of the tech sector) and towards the perceived power and irresponsibility of American 'Big Tech' companies.[6]

---

1 'UK government plans new legislation to tame internet's 'wild west'', *The Guardian,* 19 May 2018.
2 Home Office and Department for Digital, Culture, Media & Sport, Online Harms White Paper, April 2019.
3 Caroline Elsom, 'Safety without Censorship: A better way to tackle online harms', Centre For Policy Studies, 27 September 2020.
4 Damian Collins, 'Proper regulation won't suppress freedom of speech online – it will protect it', CapX, 13 January 2022
5 Online Safety Bill I 2022.
6 'Dan Milmo, 'Nadine Dorries lambasts Silicon Valley ahead of new online abuse laws', *The Guardian'*, 16 March 2022.

The resulting bill is hugely ambitious, with its 230 pages outlining a wide range of proposals addressing not only harmful online content but also fraudulent advertising. This paper is not a comprehensive analysis of the whole Bill. Rather, it is an attempt to explain the risks associated with its treatment of harmful and controversial content as well as its accompanying monitoring requirements. Because while the Government may be selling the Bill as a 'world-leading' piece of safety legislation, it is best understood as a significant threat to civil liberties, innovation and competition.

A PROBLEM IN SEARCH OF A SOLUTION

The OSB has its origins in a justifiable and praiseworthy impulse: to curb the spread of online content that has devastated lives and eroded trust. As the harms associated with such content have spread, calls for government intervention have increased. Any discussion of online speech regulation should begin with an acknowledgment of the scale of these harms, which include online harassment, political extremism, and the distribution of material involving child sexual abuse.

For example, in the UK and elsewhere around the world, women are on the receiving end of torrents of online abuse. One in five women in the UK have experienced online harassment and abuse, which can take the form of threats of violence, disclosure of intimate photos and personal information, and cyberstalking.[7] Such harassment and abuse can lead to panic attacks and persistent anxiety.[8]

Notoriously, child predators often seek targets on the Internet, and images of child sexual abuse are easily shared online. In 2021, the Internet Watch Foundation (IWF) investigated 361,000 reported incidents of child sexual abuse, noting that there has been a rise in content showing abuse of children aged between 7-10.[9] Some of the incidents IWF investigated include URLs associated with thousands of images or videos.[10]

One in five women in the UK have experienced online harassment and abuse, which can take the form of threats of violence, disclosure of intimate photos and personal information, and cyberstalking.

On the flipside, parents are understandably concerned that their young children can access online pornography. According to a survey published by British Board of Film Classification, a conservative estimate of the portion of 11- to 13-year-olds who have seen online pornography is 51%.[11] Of these children, 62% claim to have unintentionally come across pornography. The same study found that 85% of parents would like to see 'robust' age verification methods implemented in order to prevent children under the age of 18 from accessing pornography.

7 Centenary Action Group, 'End Online Abuse'

8 Amnesty International press release, 'Amnesty reveals alarming impact of online abuse against women', 20 November 2017.

9 Internet Watch Foundation, 'Three-fold increase of abuse imagery of 7-10-year-olds as IWF detects more child sexual abuse material online than ever before', 13 January 2022.

10 Ibid.

11 Department for Digital, Culture, Media & Sport, 'World-Leading Measures to Protect Children From Accessing Pornography Online', 8 February 2022.

Elsewhere on the internet, political extremists find it easy to spread their propaganda and hate. A number of online venues have become well-known as hotbeds for far-right content that encourages political violence. Such venues are also often sources of conspiracy theories such as QAnon and those associated with COVID-19 vaccines. The January 2021 assault on the US Capitol is perhaps the best example of QAnon adherents and those convinced by online election misinformation acting on their convictions.

The Online Safety Bill was therefore intended to respond to all of these concerns – and more. In the words of Matt Hancock, it would make the UK the safest place in the world to be online.[12]

WHAT THE ONLINE SAFETY BILL DOES

Duties of Care

The core of the OSB is a collection of duties imposed on 'user-to-user' (U2U) services and 'search services'. The OSB empowers Ofcom to ensure services comply with these duties, set codes of conduct and write risk assessments. U2U services include social media platforms, such as Meta and Twitter, and are defined as internet services that allow users to generate or upload content that may be encountered by another user. Search services are defined as any internet service with a search engine that allows users to query multiple websites.

Priority Illegal Content

Under the OSB, U2U services and search services must take steps to police their platforms for priority illegal content and to ensure that users do not encounter such content.[13] These obligations apply to all in-scope U2U services and search services, which by one estimate includes '20,000 micro-businesses, 4,000 small and medium businesses and 700 large businesses'.[14] The Bill defines 'priority illegal content' as terrorism content, child exploitation and abuse content as well as 'revenge porn, hate crime, fraud, the sale of illegal drugs or weapons, the promotion or facilitation of suicide, people smuggling and sexual exploitation'.[15]

However, the OSB also allows for additional content to be classified as 'priority illegal content' if the Secretary of State considers doing so appropriate because the content's prevalence amounts to an offence, the risk of harm amounts to an offence or because of the severity of the harm caused by the offence.[16]

The OSB requires search services to 'to operate a service using proportionate systems and processes designed to minimise the risk of individuals encountering [priority illegal content]'.

The obligations for U2U services and search services under this priority illegal content duty are slightly different from each other. The safety duties imposed on U2U services require (among other things) that such services 1)

12 Department for Digital, Culture, Media & Sport, 'New Laws to Make Social Media Safer', 20 May 2018.

13 s.9 (U2U) and s.24 (search services)

14 Graham Smith, 'Mapping the Online Safety Bill', 27 March 2022.

15 Department for Digital, Culture, Media & Sport and Home Office, 'Online Safety Law to Be Strengthened to Stamp Out Illegal Content', 4 February 2022.

16 s.179

'prevent individuals from encountering priority illegal content by means of the service', and 2) 'minimise the length of time for which any priority illegal content is present'.[17] The OSB requires search services to 'to operate a service using proportionate systems and processes designed to minimise the risk of individuals encountering [priority illegal content]'.[18]

Content Harmful to Adults

Those U2U services falling under OSB's 'Category 1' designation, which is expected to include the largest online platforms such as Meta and Google, will be required to explain in their terms and conditions how they will treat content harmful to adults, a category of speech that has come to be known as 'legal but harmful'.[19]

The OSB defines such content as being that 'which presents a material risk of significant harm to an appreciable number of adults in the United Kingdom'.[20] 'Harm' is defined merely as 'physical or psychological harm'.[21]

The government has been keen to argue that the provisions governing legal but harmful speech are merely transparency requirements. But as this paper will go on to explain, the provisions outlining the requirements governing 'legal but harmful' speech risk resulting in Category 1 firms removing troves of legitimate speech in an abundance of caution.

Content Harmful to Children

U2U and search services 'likely to be accessed by children' must also monitor their platforms for content that is harmful to children (again, as defined by the Secretary of State) and take steps to prevent children from accessing such content.[22] In addition, U2U and search services are required to complete risk assessments related to children's safety.[23]

U2U and search services 'likely to be accessed by children' must also monitor their platforms for content that is harmful to children (again, as defined by the Secretary of State) and take steps to prevent children from accessing such content.

Unlike the duties related to content harmful to adults, the duties governing how firms handle content harmful to children include preventing children from encountering such content.[24]

Content of Journalistic and Democratic Importance

The OSB imposes duties on Category 1 U2U and search services that are designed to protect journalistic content as well as content of democratic importance.[25]

---

17 s.9
18 s.24
19 s.12 and s.13
20 s.54
21 s.190
22 s.11 (U2U) and s. 26 (search services)
23 s.10 (U2U) and s.25 (search services)
24 s.11(3)(a)+(b) and s.26(3)(a)+(b)
25 s.15 and s.16

The journalist and democratic content duties require firms to consider 'the importance of the free expression' of such content when deciding how to moderate it and whether to take action against the user uploading or sharing the content.[26] Other duties require the services to provide an expedited complaints procedure for content if the user who shared or generated the content considers it to be journalistic content or content of democratic importance.[27]

The definition of content of democratic importance is very similar to the definition of journalistic content. It includes: 'the content is or appears to be specifically intended to contribute to democratic political debate in the United Kingdom or a part or area of the United Kingdom'.

The OSB defines journalistic content in relation to a U2U service if the content is: 1) news publisher content or user-generated content in relation to the service, 2) generated for the purpose of journalism, and 3) 'UK linked'.[28] The OSB considers content to be 'UK-linked' if: 1) 'United Kingdom users of the service form one of the target markets for the content (or the only target market)' or 'the content is or is likely to be of interest to a significant number of United Kingdom users'.[29]

The definition of content of democratic importance is very similar to the definition of journalistic content. It includes: 'the content is or appears to be specifically intended to contribute to democratic political debate in the United Kingdom or a part or area of the United Kingdom'.[30] It is these provisions which Dorries and others have pointed to in arguing that the Bill will in fact protect freedom of speech.

Criminal Offences

The OSB also introduces four new criminal offences.

1) Harmful communications: this criminalises sending a message if at the time of the sending 'there was a real and substantial risk that it would cause harm to a likely audience' and the sender of the message 'intended to cause harm to a likely audience'.[31]

   The definition of 'likely audience' includes those who might see the content after it has been forwarded or shared. 'Harm' is defined as 'psychological harm amounting to at least serious distress'. As the Centre for Policy Studies and others have warned, this potentially allows for someone to be prosecuted for online content that 'goes viral' and causes psychological distress even if neither the spread of the content nor the distress caused by the content was intended by its creator.[32] Even if no one is distressed by the content, its sender could still be in violation of the law if someone could in theory have been distressed by the content.

26 s.16(2)(a)+(b)
27 s.16(4)
28 s.16(8)
29 s.16(9)
30 s.15(6)(b)
31 s.151
32 151(3)

2) False communications: this offence criminalises sending a message that the sender knows to be false if 'at the time of sending it, the person intended the message, or the information in it, to cause non-trivial psychological or physical harm to a likely audience'.[33]

   This new law also includes the 'likely audience' requirement found in the harmful communications offence and raises the same concerns.

3) Threatening communications: under this new offence it will be a crime to send a message threatening death or serious harm if the person sending the message either i) 'intended an individual encountering the message to fear that the threat would be carried out' or ii) 'was reckless as to whether an individual encountering the message would fear that the threat would be carried out'.[34]

4) 'Cyberflashing': this criminalises sending photos or video of anyone's genitals to another person in order i) to cause alarm, distress or humiliation or ii) to obtain sexual gratification while disregarding whether the recipient will be caused alarm, distress or humiliation.[35]

   This proposal is not without potential problems. Prosecutors will have to consider the possibility that this new offence will be weaponized by vindictive former partners who claim to be victims of 'cyberflashing' when at the time the offending material was sent it was not intended to cause alarm, distress, or humiliation.

Pornography

Section 68 of OSB imposes new duties for providers of pornographic content. Among these are a duty to ensure that children are 'not normally' able to view pornographic content.[36] The OSB lists age verification as one means to satisfy this obligation, although it does not explicitly require age verification[37] The OSB also requires providers of pornographic content to keep a written record explaining what steps they have taken to fulfil this obligation while protecting users' privacy.[38]

The OSB also requires providers of pornographic content to keep a written record explaining what steps they have taken to fulfil this obligation while protecting users' privacy.

Ofcom will also provide guidance to pornographic content providers on how to comply with the child protection obligation.

RISKS TO CIVIL LIBERTIES

Speech

Arguably the single biggest problem with the OSB, although there are many, is that it provides incentives for online platforms to remove perfectly legal content. When faced with

33 s.152
34 s.153
35 s.157
36 s.68(2)
37 Ibid.
38 s.68(3)

significant fines over failure to act on content, under a regulatory scheme that includes nebulous definitions and phrases such as 'psychologically harmful' and 'appreciable number of adults', we should expect for online platforms to err on the side of caution and take down more content – especially given the eye-watering fines that they face if they do not (as discussed below).

Combined with the privacy concerns we also discuss below, the effect of the Bill will be a less private and less free online speech environment.

Above all, the OSB's design reveals a misunderstanding of how content moderation at scale works, neglecting the fact that in many cases harm associated with content is caused by the context in which the content was shared rather than the content itself.

Above all, the OSB's design reveals a misunderstanding of how content moderation at scale works, neglecting the fact that in many cases harm associated with content is caused by the context in which the content was shared rather than the content itself.

Some categories of content, such as child pornography, are illegal regardless of context. Large technology firms already take steps to identify this content by using technology such as PhotoDNA, which assigns hashes (i.e. digital fingerprints) to illegal content, thereby allowing for its automated detection, removal, and reporting. The same technology can be used to identify other content. But for content that is not specifically illegal, removal will hinge on context.

For example, Meta's bullying and harassment policy notes: 'We allow people to post and share if it is clear that something was shared in order to condemn or draw attention to bullying and harassment.'[39] Accordingly, footage of students bullying a classmate may be removed in one instance (eg if posted by one of the bullies) or kept online in another (eg if posted by an anti-bullying charity to highlight the need for schools to take more steps to tackle bullying). Meta's policies reflect an understanding that a policy of 'no footage of bullying' is not an optimal policy.

Policies associated with other kinds of content that sound at first glance reasonable, such as 'no images of nude children', can also result in unintended consequences. In 2016, Meta removed the Pulitzer Prize-winning photograph 'The Terror of War'. The photo, by Nick Ut, is one of the most recognisable images of the 20th century, showing children fleeing a South Vietnamese napalm attack in 1972. One of the children in the photo, a burnt nine-year-old girl, is naked.

Meta removed the photo from a number of accounts, including the account of the naked girl in the picture.[40] In the wake of widespread uproar, it was reinstated. But such decisions are being made thousands of times a day, often without any accompanying scrutiny.

---

39 Meta, 'Bullying and Harassment'

40 Terje Solsvik, Yasmeen Abutaleb, 'Facebook reinstates Vietnam photo after outcry over censorship', Reuters, 9 September 2016.

Examples such as the Ut photo highlight why the OSB's obligations are destined to have a chilling effect on online speech. As noted above, the OSB criminalises sending 'harmful' content regardless of whether the offended party was the intended audience or whether the sender intended harm. Under the OSB, U2U and search services would have to comply with Ofcom guidance on dealing with such harmful content. Absent context being appropriately considered, we should expect U2U and search services to remove content of historic, artistic, educational and documentary significance.

Imagine, for sake of argument, that a Ukraine-based user of the hypothetical social media platform VidNet uploaded a video of alleged Russian atrocities. Under the OSB, VidNet would have to consider whether the video was likely to cause harm, regardless of whether harm was intended. It would not matter that the video had been shared to a group dedicated to tracking Russian war crimes, or that no one had complained about the content to the social media company. VidNet would also have to consider whether there was a good reason for uploading the video and whether it constituted journalistic content or content of democratic importance.

Then, if a Vidnet user did inform Vidnet that they were distressed by the video, Vidnet would have to determine whether such a user would be part of the 'likely audience' of similar content and whether such content was likely to result in harm. In such a regulatory environment, online services will be heavily incentivised to limit access to legal content, thereby stifling debate, education, activism and commentary.

The Government argues that the 'harmful to adults' content obligations are not designed as a backdoor censorship regime, but instead as a means to encourage transparency over the terms and conditions of content moderation. Yet to avoid civil (and potentially criminal) consequences over perceived inaction, we should expect large firms to design content moderation systems that embrace the possibility of false positives and take down troves of legal speech.

The Government argues that the 'harmful to adults' content obligations are not designed as a backdoor censorship regime, but instead as a means to encourage transparency over the terms and conditions of content moderation.

This is all the more so given the eye-watering nature of the potential fines if these firms are judged to be breaching the rules.

The OSB requires Category 1 services to explain in their terms of service how they will treat 'legal but harmful' speech. They can choose to take down the content, restrict user access to the content, or limit its recommendation or promotion.[41] The Bill leaves Category 1 services free to 'recommend or promote' legal

41 s.13

but harmful speech. However, given that the largest social media firms already take steps to moderate speech that is likely to be included in the 'legal but harmful' category (such as misogynistic abuse or content associated with eating disorders) it is unlikely that they will choose to recommend or promote such content. They will therefore be put in a position of pledging to moderate such content and facing significant fines if they fail to act on it swiftly. Indeed, OSB's mandates are backed by fines of up to 10% of annual global revenue or £18 million (whichever is greater).[42] Given the prospect of a multi-billion-pound fine, Category 1 services are likely to err on the side of caution and embrace false positives as the price of compliance – whatever theoretical provisions the Bill contains about free speech. The balance of incentives is blindingly obvious.

The results of the journalistic and democratic importance provisions are likely to include a number of unintended consequences including but not limited to valuable news sources enjoying fewer protections than 'news publisher content' as defined in the Bill.

Supporters of the OSB might claim, and even believe, that the Bill's provisions related to journalistic content and content of democratic importance provide a bulwark against censorship or the erosion of free speech online. Yet these provisions are themselves unfair: they create an online speech environment where whoever is deemed by the state to be producing 'journalistic' content or 'content of democratic importance' will enjoy more protections from the largest online firms than other users.

Nadine Dorries insists that the OSB is not a threat to free speech thanks to a provision of the Bill that imposes a duty on affected services to 'have regard to the importance of protecting users' right to freedom of expression within the law'.

Furthermore, the definitions of 'journalistic' content and 'content of democratic importance' are so vague as to exclude whole swathes of content. Are TikTok videos created by a Ukrainian civilian showing her and her friends climbing the wreckage of Russian tanks 'generated for the purpose of journalism'? What about confidential government documents posted on Wikileaks? What is included in 'democratic political debate'? Are the beliefs that racial minorities should be banned from voting, or the outlawing of a religion, included?

The results of the journalistic and democratic importance provisions are likely to include a number of unintended consequences including but not limited to valuable news sources enjoying fewer protections than 'news publisher content' as defined in the

42 Schedule 13(4)

Bill. This is especially concerning given that most young people in the UK do not consume news content on traditional media platforms such as TV, newspapers and radio as much as their older peers. They prefer getting their news from social media and other internet platforms, which are excluded from the definition of 'news publisher content'.[43]

This is something that should particularly worry Conservative MPs. At the moment, many of them appear to be inclined towards the Bill because they believe it will help curb the amount of abuse that they personally receive online. As mentioned above, the volume of online abuse is certainly horrendous – particularly that directed at female MPs. But what politicians do not seem to have realised is the potential for these rules to be used, under a different Government, to stifle their own free speech. It is easy to see how certain views on the hot-button social issues of the day – while perfectly legal to hold – would be judged harmful by many of those in a position to read them, for example on the ethics of assisted dying, or gay marriages taking place in church, or the difference between sex and gender.

Nadine Dorries insists that the OSB is not a threat to free speech thanks to a provision of the Bill that imposes a duty on affected services to 'have regard to the importance of protecting users' right to freedom of expression within the law'.[44] But the OSB will simultaneously make it too risky for firms to tolerate a wide range of speech. Far from protecting users' freedom of expression, the Bill will result in less legal speech appearing online.

Privacy

While its effect on free speech is the main problem with the OSB, it is far from the only one. The OSB also encourages online services to weaken privacy protections and to closely monitor their users. For example, it requires online services that allow users to upload or view pornography to take steps to ensure that children cannot access pornographic content – a worthy goal, but one that also incentivises online services to weaken encryption and collect more personal information on users, thereby putting them at increased risk of blackmail, surveillance and identity theft.

While its effect on free speech is the main problem with the OSB, it is far from the only one. The OSB also encourages online services to weaken privacy protections and to closely monitor their users.

In fact, the OSB also contains more general incentives for tech firms to step up the monitoring of users' communications.

The UK is no longer bound to the EU's Electronic Commerce Directive, which provides protection against general government

43 Ofcom, 'News Consumption in the UK: 2022', 21 July 2022.

44 s19. Matt Dathan, 'Frontrunner Liz Truss will pursue online safety, says Nadine Dorries', The Times, 29 July 2022.

monitoring obligations.[45] This weakens privacy even as the OSB encourages firms to step up their proactive surveillance for 'priority illegal content' – which the Secretary of State can change the definition of . In other words, the OSB has the potential to require online services to proactively monitor their users for any content that might cause offence. Such a move would put both user privacy and speech at risk.

The OSB also requires U2U services to ensure that users do not encounter priority illegal content. Given that terrorists and other criminals are known to use encrypted services, it is reasonable to view the OSB as a threat to encrypted communication services.

However, the most alarming privacy concern associated with the OSB is that the Bill encourages providers of encrypted communications systems to weaken encryption or remove these systems altogether. Section 104 empowers Ofcom to require U2U services to 'use accredited technology to identify terrorism content communicated publicly by means of the service and to swiftly take down that content'.[46] The OSB also requires U2U services to ensure that users do not encounter priority illegal content.[47] Given that terrorists and other criminals are known to use encrypted services, it is reasonable to view the OSB as a threat to encrypted communication services.

Encrypted communication systems such as WhatsApp and Signal allow users to communicate with each other using 'end-to-end encryption' (E2EE). Such encryption ensures users that third parties (including the E2EE provider) cannot read the messages sent between users. Under the OSB, WhatsApp and Signal are U2U services. As such, they will be required to prevent users from encountering 'priority illegal' content and remove such content when made aware of it. It is impossible for E2EE providers to fulfil this obligation. E2EE is designed so that providers cannot monitor communications or remove it.

This is especially concerning given that E2EE communications are crucial for journalists, activists, whistleblowers, and many others.

---

45 'Member States shall not impose a general obligation on providers, [...] to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.'

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000.

The Government's OSB explanatory notes explain in paragraphs 28 and 29:

'28. The eCD prevented member states from imposing liability on service providers who provide a service that 'consists of the storage of information provided by the recipient of the service' for content created by users, so long as 'the provider does not have actual knowledge of illegal activity or information and ... is not aware of facts or circumstances from which the illegal activity or information is apparent'. This limitation was contingent on the host, upon gaining knowledge of such content, removing it expeditiously. Article 15 of the eCD also contained a prohibition on the imposition of requirements on service providers to generally monitor content they transmit or store, or to actively seek facts or circumstances indicating illegal activity.

29. The status of the eCD following the United Kingdom's exit from the EU is governed by the European Union Withdrawal Act 2018 (EUWA), which contains some provision for the continued operation of EU law. Section 5 of the EUWA holds that the supremacy of EU law ceased following the end of the transition period. This means there is no longer a legal obligation on the United Kingdom to legislate in line with the provision'.

Online Safety Bill Explanatory Notes, 11 May 2022.

46 s.104(2)(a)

47 s.9(3)(a)

E2EE ensures that sources can communicate with journalists secure in the knowledge that their messages cannot be intercepted by law enforcement, employers, or national intelligence agencies.

Communities that have often found themselves on the receiving end of government surveillance, such as racial, political and sexual minorities, often use encrypted communication channels to organise legal political activities. Many victims of domestic abuse and stalking also use encryption to conceal their communications from abusers and stalkers.[48]

Faced with OSB obligations to monitor platforms, we should expect encrypted services to cease operation in the UK if the Bill becomes law. The CEO of WhatsApp has already noted that the company will not weaken its security in light of government mandates.[49] This may sound hyperbolic, but there is precedent for encrypted services ceasing operation rather than compromising their products in the face of government pressure. Lavabit, the email service Edward Snowden used to communicate his leaked documents to journalists, chose to shut down rather than reveal its private keys to the US federal government.[50] Shortly afterwards, Silent Circle, an encrypted communications service, shut down its encrypted email service.[51] Encrochat, a firm that sold encrypted phones, closed after reports revealed that law enforcement had been hacking its customers (who admittedly appeared to have included most of Europe's leading mobsters).[52]

Faced with OSB obligations to monitor platforms, we should expect encrypted services to cease operation in the UK if the Bill becomes law. The CEO of WhatsApp has already noted that the company will not weaken its security in light of government mandates.

Some might argue that E2EE providers could comply with the OSB without putting users' privacy at risk by using a 'backdoor' key that only police and national intelligence agencies can access. This is an unrealistic expectation. A 'backdoor' key would become the target of adversarial foreign intelligence agencies and criminals, exposing police and intelligence agency officials to potential hacks and blackmail. Building a 'backdoor' encryption key would compromise millions of Britons' privacy and put national security at risk.

It is also important to point out that it is already possible for encrypted services to report illegal and abusive content. For example, Facebook Messenger allows users to encrypt their communications.[53] Meta, which owns Facebook, cannot access these communications.

48 Anna Higgins, 'How Strong Encryption Can Protect Survivors of Domestic Violence', Internet Society, 18 December 2020.

49 Shiona McCallum, 'WhatsApp: We won't lower security for any government', BBC News, 30 July 2022.

50 Kim Zetter, 'A Government Error Just Revealed Snowden Was the Target in the Lavabit Case', *Wired*, 17 March 2016.

51 Hayley Tsukayama, 'Lavabit, Silent Circle shut down e-mail: What alternatives are left?' *The Washington Post*, 9 August 2013.

52 Joseph Cox, 'Encrypted Phone Network Says It's Shutting Down After Police Hack', Vice, 22 June 2020.

53 Facebook Messenger Help Center, 'End-to-end encryption on Messenger'.

However, Facebook Messenger also uses message franking technology, which allows users to report abusive or illegal material in Messenger communications to Meta without compromising the security of their messages.[54] While such technology does allow access to encrypted messages, it nonetheless relies on users reporting the offensive or illegal content. As such, it would not satisfy a general monitoring obligation.

As one security researcher noted, the OSB could drive more people (including children) to the dark web, where they will be more likely to access not only pornography but a wide range of illegal content.

Among the other concerning provisions associated with the OSB are those related to pornographic content. In order to be effective, the age assurance systems that pornographic content providers implement will pose a significant risk to users' privacy.

'Age assurance' could require that users merely affirm that they are adults when visiting pornographic websites or enter their date of birth. Such a system is not hard for children to circumvent, so it is possible that Ofcom's guidance on child protection will require that users submit documentation (e.g. a photo of a driver's licence) as part of the age verification process.[55] Indeed, the Bill lists age verification as a method that would satisfy the child safety requirement.[56]

Such documentation could put users at risk of having their identity linked to pornographic content, leading to possible social sanction, blackmail and identity theft. Criminal hacks of pornographic website data have occurred before, and we should expect pornographic websites to become increasingly attractive targets for criminals and foreign adversaries if they know such sites collect personal information associated with users.[57]

Aside from the risk of criminal hacks, there is also the risk of inadvertent leaks, which pose the same risk to user privacy. These risks are too significant for a policy that children will almost certainly be able to circumvent easily: it is not difficult for teenagers to access virtual private networks or web browsers such as Tor that allows users to conceal their identity and location. As one security researcher noted, the OSB could drive more people (including children) to the dark web, where they will be more likely to access not only pornography but a wide range of illegal content.[58]

And again, there are other solutions already in place. Major technology firms such as Apple, Google, Microsoft and many others allow for parents to limit children's access to pornographic sites. Such parental control measures are not perfect, but lawmakers should be wary of letting the perfect be the enemy of the good, especially when the privacy

54 Seny Kamara, Mallory Knodel, Emma Llansó, Greg Nojeim, Lucy Qin, Dhanaraj Thakur, Caitlin Vogus, 'Outside Looking In: Approaches to Content Moderation in End-to-End Encrypted Systems', Center for Democracy and Technology, August 2021.

55 S68: 'A duty to ensure that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service (for example, by using age verification).'

56 s.68

57 'Porn website hacked, 72,000 usernames stolen', NDTV, 14 March 2012.

58 Chris Summers, 'UK Online Safety Bill Could 'Drive More People Into the Dark Web'', *The Epoch Times*, 29 April 2022.

of millions of law-abiding British citizens and residents is at stake.

COMPETITION AND INNOVATION

The final major criticism of the OSB is that it will hamper competition and innovation. This is thanks to the range of costs associated with compliance with OSB's obligations, which are expected to be extremely significant.

In 2020, the Department for Digital, Culture, Media and Sport commissioned a consulting firm to estimate the compliance costs associated with the OSB as part of the Bill's Impact Assessment (IA).[59] According to the IA, familiarisation with the OSB will cost British businesses £2.5 billion over 10 years.[60] However, as the Institute of Economic Affairs' Matthew Lesh and Victoria Hewson have noted, this is likely a significant underestimate.[61]

Such costs could reduce what has been a welcome increase in technology investment in the UK over the last few years. Between 2016-2020, foreign investment in British technology firms increased from about £3 billion a year to almost £10 billion a year.[62] Domestic investment has also increased, rising from £3 billion a year to more than £5 billion in the same time period.[63] Post-Brexit, the government has the opportunity to develop a policy framework that makes the UK look more attractive to foreign investors and maintains its position as one of the globe's leading technology and innovation hubs.

Unfortunately, the OSB will increase the costs to firms seeking to do business in the UK and expose them to extensive civil and criminal liability. We should expect many foreign investors and businesses looking to expand to prioritise growth in the EU market before the UK. Indeed, this is precisely what technology firms and investors have been warning about.

Between 2016-2020, foreign investment in British technology firms increased from about £3 billion a year to almost £10 billion a year.

This effect will affect far more than the social media websites. Although 'Big Tech' giants such as Meta, YouTube, and Twitter are often the focus of discussions around the OSB, the legislation's definition of 'U2U' services will go far beyond social media platforms. Online dating apps, ride sharing platforms, food review websites, academic research databases, online encyclopaedias, e-commerce platforms, live-streaming services, cloud file storage systems and many, many others will be within OSB's scope. Any investor in a company or industry in the UK that allows users to upload content, whether a social media service or not, will have to consider the costs associated with OSB. And of course, powerful market incumbents have the resources to pay these costs and will benefit from smaller competitors struggling to do so.

59 Online Safety Bill Impact Assessment.

60 Ibid.

61 Matthew Lesh and Victoria Hewson, 'An Unsafe Bill: How the Online Safety Bill Threatens Free Speech, Innovation and Privacy', Institute of Economic Affairs, 27 July 2022.

62 Tech Nation, 'The Future UK Tech Built', 2021.

63 Ibid.

A WAY FORWARD

Throughout his years as leader of the Conservative Party, David Cameron was a consistent critic of quangos such as Ofcom. Indeed, the 2010 Conservative Party manifesto bemoaned the 'explosion of unaccountable quangos'. A year before the 2010 general election, Cameron pledged to reduce Ofcom's powers 'by a huge amount'. But Ofcom's powers were not seriously curtailed – in fact, under Cameron they grew to encompass the regulation of postal services.

Now, however, the Conservative Party is proposing the most extraordinary expansion of the quangocracy – to give Ofcom day-to-day oversight of what millions of us say to each other online, with the big tech firms as its conscripted enforcers.

During the 2021 Conservative Party Conference government ministers bemoaned the rise of 'cancel culture' and 'woke aggression', with then-Foreign Secretary Liz Truss insisting: 'We reject the illiberalism of cancel culture'.

The irony is that this comes even as the Government has professed its concern over the restriction of free speech. The introduction of the Higher Education Bill (HEB) suggests that the Government is aware of worries that universities are not the bastions of free speech and open inquiry that many expect.[64] During the 2021 Conservative Party Conference government ministers bemoaned the rise of 'cancel culture' and 'woke aggression', with then-Foreign Secretary Liz Truss insisting: 'We reject the illiberalism of cancel culture'.[65]

Yet the OSB would worsen the sorry state of free speech in the UK – and hand those keen to stifle speech an extraordinarily powerful weapon, especially under a government of a different political complexion.

Sadly, the OSB is just the latest development in the trend of using the heavy hand of the state to address offensive speech. Indeed, for decades, the British government's response to offensive speech has been to criminalise it, with British citizens already facing jail sentences and fines for online speech.[66] And rather than taking a robust stand for freedom of speech, the Government is now set to pass a law that will empower politicians across the spectrum to stifle expression.

We believe that British civic institutions are robust enough to function as venues of debate on the difficult and often emotional issues surrounding race, sexuality, politics, religion and other important topics. The UK boasts some of the world's leading universities, journalistic outlets, and other civic institutions where such issues are often discussed. In a liberal democratic society such as the UK, it is these civic institutions, not the state, that are best-positioned to be venues where citizens can

64 Higher Education (Freedom of Speech) Bill I 2022

65 Rowena Mason, Jessica Elgot and Aubrey Allegretti, 'Conservatives Take Aim at Cancel Culture and 'Woke Aggression'', 3 October 2021.

66 'Man who sent Marcus Rashford racist Euro 2020 final tweet jailed', BBC News, 30 March 2022.

'Man fined for hate crime after filming pug's 'Nazi salutes'', BBC News, 23 April 2018.

Sam Hancock, 'Man charged over 'offensive' tweet about Captain Sir Tom Moore', *The Independent*, 10 February 2021.

discuss these topics. In the last few decades social media has emerged as one of these institutions. That content on such platforms is sometimes offensive and harmful should not prompt lawmakers to reach for the kind of state action outlined in the OSB. Because in this case, the cure is very much worse than the disease.

In an ideal world, the Government would scrap the OSB in its entirety. Absent scrapping the Bill, we strongly urge ministers to remove the most alarming elements from it, as highlighted by the CPS and other civil liberties campaigners.

In particular, the Government should remove any obligations associated with legal content. The 'legal but harmful' elements of the OSB are a significant threat to free speech and competition. If Members of Parliament believe that content is so harmful that it ought to be removed from the internet, then they should make their case in Parliament and introduce legislation criminalising such content.

The Government should also take steps to ensure that E2EE remains secure and available to British residents. The OSB should state clearly that no services that provide E2EE shall be compelled to weaken their encryption. Mandating the monitoring of user communications jeopardises the privacy and security of law-abiding British citizens and residents.

The OSB's pornographic content provisions also have the potential to put privacy at risk. The Government should amend the Bill in order to clarify that no provider of pornographic content will be compelled to store personal identifiable information related to visitors.

But the Government can go further than scrapping OSB or making significant amendments to it. It could switch to a better approach: legislation that provides comprehensive online intermediary liability protections. Section 230 of the United States' Communications Decency Act, sometimes referred to as the '26 words that created the internet', ensures that interactive computer services of any size cannot face civil suit over decisions associated with removal of users' content, regardless of what motivated such removal.

In an ideal world, the Government would scrap the OSB in its entirety. Absent scrapping the Bill, we strongly urge ministers to remove the most alarming elements from it, as highlighted by the CPS and other civil liberties campaigners.

A British version of such legislation would not only provide legal clarity for a popular industry, but it would also level the playing field, thereby allowing online services in the UK to develop tools and methods for content moderation without the fear of costly litigation associated with content removal decisions. Like Section 230, the legislation could still allow for users to file suits related to illegal speech and content that violated copyright law.

CONCLUSION

The Online Safety Bill is designed to address genuine challenges. And it does have good features, such as the decision to judge online services based on their overall content moderation regime rather than second-guessing specific decisions.

But at the same time, this messy, sprawling and complex piece of legislation will have a chilling effect on free speech, on online privacy, and on the UK tech sector. We urge the new Government to ditch it for good.

ABOUT CPS

The Centre for Policy Studies is one of the oldest and most influential think tanks in Westminster. With a focus on taxation, economic growth, business, welfare, housing and the environment, its mission is to develop policies that widen enterprise, ownership and opportunity. As an independent non-profit think tank, the CPS's work is supported by likeminded individuals and companies, but it retains full editorial control of all output to ensure that it is rigorous, accurate and unbiased. Founded in 1974 by Sir Keith Joseph and Margaret Thatcher, the CPS has a proud record of turning ideas into practical policy. As well as developing the bulk of the Thatcher reform agenda, it has been responsible for proposing the raising of the personal allowance, the Enterprise Allowance and the ISA, as well as many other more recent successful policy innovations, such as increasing the National Insurance threshold, free ports, fixed-rate mortgages, full expensing, the public sector pay freeze, the stamp duty holiday, and putting the spotlight on how to use market-based solutions to reach Net Zero targets.

ABOUT THE AUTHOR

Matthew Feeney is the Head of Technology and Innovation at the Centre for Policy Studies. He was previously the director of the Cato Institute's Project on Emerging Technologies.

ISBN: 978-1-914008-27-6
September 2022