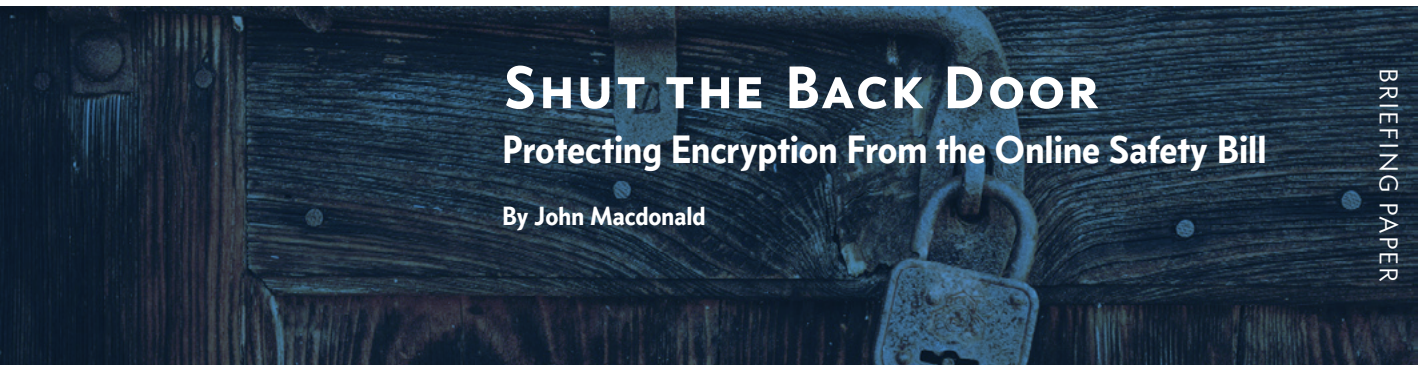

Shut the Back Door

Protecting Encryption From the Online Safety Bill

By John Macdonald

BRIEFING PAPER

EXECUTIVE SUMMARY

- End-to-end encryption is foundational to the proper functioning of our online experience;
- The Online Safety Bill would—in its current form—undermine end-to-end encryption by empowering Ofcom to demand service providers use 'accredited technology' to give them access to encrypted content in certain circumstances, under threat of large fines;
    - The Bill also grants the Secretary of State sweeping discretionary powers to determine the scope of services included in such provisions;
- Undermining end-to-end encryption poses a grave threat to privacy, security and the wider UK economy;
    - There is no sense in which encryption could be maintained while another party not participating in the information exchange has access to the contents;
    - Creating an encryption 'backdoor' for law enforcement would effectively be a blackmailer's charter, allowing criminals and hostile foreign actors to exploit security flaws;
    - Such measures would undermine the growth and competitiveness of the UK technology sector, potentially resulting in large companies withdrawing from the market entirely;
- Weakening encryption undermines the credibility of the UK on the international stage, providing tacit justification for oppressive regimes like Russia and China to violate civil rights;
- Despite Government protestations to the contrary, the use of 'client-side scanning' would not address privacy concerns, as demonstrated in the school safety sector;
- The Government should redraft the Online Safety Bill to ensure end-to-end encryption is properly protected;
- Certain elements of the Bill should be removed entirely, including:
    - Clause 104(2) which allows Ofcom to issue a notice requiring service providers to use 'accredited technology' to identify and 'deal with' content deemed harmful;
    - Clause 92(4) which makes it an offence for the provider to give 'information which is encrypted such that it is not possible for Ofcom to understand it, or produces a document which is encrypted such that it is not possible for Ofcom to understand the information it contains';

ADAM SMITH INSTITUTE – THE FREE-MARKET THINKTANK
23 Great Smith Street,
London, SW1P 3BL
+44 (0)20 7222 4995
www.adamsmith.org

- Schedule 12 which further stipulates that failure to comply can lead to fines of up to £18 million or 10% of global revenue;
- The Government should also undertake a review of client-side scanning technologies, to better understand the tradeoffs between privacy and security that their implementation brings.

ABOUT THE AUTHOR

John Macdonald is Director of Strategy at the Adam Smith Institute.

End-to-end encryption (henceforth referred to as encryption[1], for brevity) is foundational to the proper functioning of our online experience. For secure banking to messaging services like WhatsApp, encryption is part of the fundamental architecture that makes these services work. However, like the structural foundations of a building, its significance is often lost on us without active attention. But if we were to undermine it, much of what we take for granted online would be severely compromised, or in some cases, impossible.

For now, WhatsApp, Signal, Zoom and other communication services that have implemented encryption can reasonably claim that *only the intended recipients of a communication can view them.*

However, the Online Safety Bill (OSB) empowers Ofcom to compel service providers to use "accredited technology" to identify harmful content and "swiftly take down that content" given their "duty of care"[2]. It also grants the Secretary of State for the Department of Digital, Culture, Media and Sport (DCMS) the power to add or remove services from an exemption list and to place particular service providers into one of four broad categories administered by Ofcom;

(1) all providers of regulated user-to-user services;

(2) services likely to be accessed by children;

(3) services with additional duties to protect journalistic content and "content of democratic importance";

(4) search engine providers.

While these categories are designed and administered by Ofcom, the Bill also transfers an unprecedented amount of power to the Secretary of State. For example, they will be able to define priority content considered harmful to children and adults in secondary legislation (section 53).[3] They would also have the power to set out the Government's strategic priorities in relation to online safety matters, which Ofcom will have to consider (section 78).

The intention behind the Bill is to make the UK the 'safest place in the world to be online while defending free expression."[4] In practice, this effectively places a

---

1 End to end encryption occurs when the sender or creator encrypts data, and only the intended receiver or reader can decrypt it. It is more secure than mere encryption in transit, for example, in which data is only encrypted on the server side.

2 Internet Society, 'Internet Impact Brief: End-to-end Encryption under the UK's Draft Online Safety Bill', January 2022: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/

3 Article 19, 'UK: Online Safety Bill is a serious threat to human rights online', April 2022: https://www.article19.org/resources/uk-online-safety-bill-serious-threat-to-human-rights-online/

4 DCMS, 'Online Safety Bill: factsheet', April 2022: https://www.gov.uk/government/publications/online-safety-bill-supporting-documents/online-safety-bill-factsheet

burden on service providers and platforms to implement either of these options under Ofcom's direction with significant influence from the Secretary of State. Where they feel it appropriate, they will have the power to compel companies to use "proactive technology [including] content moderation technology, user profiling technology or behaviour identification technology which utilises artificial intelligence or machine learning."[5]

Encryption, and more broadly genuinely secure and private exchange, underpins the social norms of modern communication and commerce. Weakening it risks not only economic harm, but would undermine our fundamental right to privacy and cause great damage to the way we interact with one another. Our recommendations in this paper are simple. Remove clauses that transfer unchecked power to the Secretary of State that can be used to compel companies to violate the privacy of exchange between individuals, and build in legal protections for the implementation of end to end encryption.

THIS IS ABOUT PRIVACY, NOT JUST TECHNOLOGY

End to end encryption should be defined relative to how well it achieves its end: separating entities which know the *key*, and thereby are enabled to read, possibly write, reply, amend, or elide certain content, from *anyone else.*[6] Its fundamental purpose is to prevent the contents, or knowledge about the contents, of an interaction between individuals from becoming known by another party.

We should reframe the debate around the purpose of encryption, rather than the technology itself. Encryption is just a means, it has no political value in and of itself. Focusing on it means we get sidetracked into discussions about what the technology is, how it works, whether or not it could *technically* be maintained while finding ways to access data that would otherwise be private.

This becomes obvious when we look at the ways to maintain encryption but acquire access to private exchanges which are currently being explored by the government (like client-side scanning or 'CSS'). Far from being the means by which our privacy is protected, it provides cover for the government to interfere with privacy while claiming to respect it: a way to say that they split the difference between privacy and safety, that encryption has been maintained *and* that law enforcement has what it needs to protect people from harm.

When discussing technologies like encryption and CSS, we should avoid being drawn into technicalities and navel gazing around definitions. They should be referred to in the context of the effect they have on privacy, safety and security, rather than the precise ways in which they function.

---

5 UK Parliament publications & records, 'Online Safety Bill [as Amended in Public Bill Committee]', August 2022 (pg.151 152): https://publications.parliament.uk/pa/bills/cbill/58-03/0121/220121.pdf

6 Dropsafe, 'A Civil Society Glossary and Primer for End-to-End Encryption Policy in 2022', July 2022: https://alecmuffett.com/alecm/e2e-primer/e2e-primer-print.html#the-purpose-of-encryption

The purpose of encryption is to preserve a 'field model' of privacy for participants online.[7] Put simply, this suggests encrypted, private communication should be as if the participants were conducting their conversation in a field. The implication is that participants will have volunteered themselves into this situation, in which they are audibly isolated from external parties. It might be that observers can *see* a conversation is taking place, at a certain time, between a number of identifiable individuals, for a certain duration. But the contents of those interactions remain unknown.

Focusing on privacy in this way, rather than on the technicalities of encryption is extremely important from a civil liberties perspective. Advocates for trading privacy off for safety do so on the argument that it is proportionate to the vastly expanded means we have available to communicate with each other. They say it is inappropriate that people can instantaneously and privately share communications across the globe, without the prospect of interference from a third party.

But this has long been the case.[8] Governments should choose to recognise private communication as *mundane*, something easily accomplished in person by moving to a private space. Given that the UK has freedom of association, the government should also accept and protect the fundamental right of individuals to communicate freely and privately, regardless of the technological means.

HOW DOES THE ONLINE SAFETY BILL THREATEN PRIVACY AND SECURITY?

The Bill has wide-ranging implications for end-to-end privacy. Clause 104(2) allows Ofcom to issue a notice requiring service providers to use 'accredited technology' to identify child abuse content, whether communicated publicly or privately.

Clause 92(4) then makes it an offence for the provider to give 'information which is encrypted such that it is not possible for Ofcom to understand it, or produces a document which is encrypted such that it is not possible for Ofcom to understand the information it contains'. Schedule 12 of the Bill stipulates that failure to comply could lead to fines of up to £18 million or 10% of global revenue (whichever amount is greater).

Put simply, this regulatory framework and penalty system puts an onus on companies to either weaken encryption or provide other means by which to access private exchanges. Lawmakers have claimed that the Bill does not remove the end-to-end encryption[9] as it simply requires companies to install 'encryption backdoors' to allow 'exceptional access' to law enforcement agencies.

---

7 Ibid.

8 Wikipedia, 'Crypto Wars': https://en.wikipedia.org/wiki/Crypto_Wars

9 Internet Society, 'Internet Impact Brief: End-to-end Encryption under the UK's Draft Online Safety

An encryption backdoor is oxymoronic; encryption by definition does not allow third parties to hold a key to a conversation. There is no sense in which encryption could be maintained while another party not participating in the information exchange has access to the contents.

What does this mean in practice?

This is not just a matter of violating privacy. Creating a backdoor for law enforcement will also create an opening for criminals and hostile actors to exploit. For example, in 2015 Juniper Network Inc.[10] discovered an unauthorised code in their firewall ScreenOS that allowed hackers to decipher encrypted information to gain access to the network of their customers. A probe into the cause suggested that *there was an intentional flaw in the encryption algorithm* Dual_EC, enabling the US National Spy Agency to eavesdrop on overseas clients of Juniper.[11] The opening rendered the system as vulnerable to cyberattacks as it was to the NSA.

The extremely broad discretionary power given to the Secretary of State only adds to the security risk. The government might assure the public that email services, at least for now, are exempted from the Bill. However, *clause 174(9)* empowers the Secretary of State to add or remove services from the exemption list, so the scope of the legislation might broaden in the future with little oversight. This would create a chilling effect; service providers who are currently exempted might opt to weaken encryption to conform to the potential effects of the Bill in the future. It also creates completely arbitrary criteria by which a Secretary of State decides what is exempted, opening them up to special pleading from various service providers, each making the case that their services are more in need of exemption than the next.

Why there can be no 'splitting the difference' between privacy and security

Client Side Scanning (CSS) has been posited as a means to overcome the risks associated with compromised encryption. As has been made evident, it is not possible to simply provide keys, backdoors or vulnerabilities to law enforcement to allow them to bypass it without opening people to greater risk from bad actors. Client Side Scanning attempts to avoid this by acquiring and transmitting only the relevant data to the relevant parties and so would not require a direct compromise of data security. It technically allows for end to end encryption[12], but completely undermines end to end *privacy,* because messages are being scanned for content.

Bill', January 2022: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/

10 Bloomberg UK, 'Juniper Breach Mystery Starts to Clear With New Details on Hackers and U.S. Role', September 2021: https://www.bloomberg.com/news/features/2021-09-02/juniper-mystery-attacks-traced-to-pentagon-role-and-chinese-hackers

11 Reuters, 'Spy agency ducks questions about 'back doors' in tech products', October 2020: https://www.reuters.com/article/us-usa-security-congress-insight-idUSKBN27D1CS

12 Abelson et al., 'Bugs in our Pockets: The Risks of Client-Side Scanning', October 2021 (pg.1): https://arxiv.org/abs/2110.07450

CSS works by constantly scanning information (texts, videos, audio, etc.) against certain criteria, all from within the software architecture of the app or device being used, as opposed to external servers. If there is a match, the data will be flagged and made available to examination by law enforcement should they be interested. The purpose here is that all information remains encrypted, *unless* CSS software running on the device itself flags something.

Its mechanism of operation is similar to that of antivirus software. AV software has access to the entire operating system, and will scan files against its own checklist to see if they have been compromised. It runs in the background, often completely unbeknownst to the user. By putting its implementation at the discretion of a Secretary of State, the only barrier between scanning illegal content such as child sexual abuse material ('CSAM') or planned criminality, and scanning for 'legal but harmful content' is a political one.

Given that the Bill, in its current draft, intends to compel online platforms to monitor, evaluate and potentially remove 'legal but harmful' content expressed publicly, it is entirely possible this could be extended to private communications. This might be done on the grounds that people who discuss certain topics in a particular way are more likely to commit related offences, and that law enforcement access could prevent crime.

The point is not that this will happen, merely that it could. The Bill does not have sufficient protections for encryption or privacy within it. Avoiding this situation is almost entirely at the discretion of the Secretary of State, rather than being enshrined in law.

Error rates and accountability

It is important to bear in mind that, much like encryption backdoors, CSS cannot be targeted in a way that does not compromise the security or privacy of the user. Apple's proposed CSS solutions, "are notoriously unreliable and prone to mistakenly flag art, health information, educational resources, advocacy messages, and other imagery".[13]

Apple later retracted this proposal due to the inherent risks to privacy and security that would have arisen from the implementation of such a policy. Far from protecting children, such a requirement would compel providers of services, both large and small, to introduce vulnerabilities into their platforms that jeopardise not only device security but place the rights of all users, including children, at grave risk.

CSS cannot be perfect. It is subject to algorithmic bias[14], and crucially cannot screen for context. This means that family moments, like a mother sending a video

---

13 Global Encryption Coalition, '45 organizations and cybersecurity experts sign open letter expressing concerns with UK's Online Safety Bill', April 2022: https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/

14 Abelson et al., 'Bugs in our Pockets: The Risks of Client-Side Scanning', October 2021 (pg.19): https://arxiv.org/abs/2110.07450

of her child to their grandmother, or private exchanges between queer kids[15] could be sent to law enforcement. While the error rate can be trimmed down through training and optimisation, part of this process involves human interaction to train out images from non-relevant contexts, exposing non-threatening content sent with greatest intended privacy to outside parties for scrutiny.

These scenarios are entirely in keeping with reality, and have played out at a much smaller scale in schools as a result of 'safety tech'.

The scaling up of school 'safety' tech

Given that the Online Safety Bill allows the Secretary of State to mandate the building of a backdoor, or implementation of a silent observer or CSS, it stands to reason that this could create a two-track 'splinternet', in which online access and experience is vastly different between children and adults. This might sound far-fetched, but such a system has been explicitly endorsed by the Prime Minister Liz Truss, and is therefore a fairly likely outcome should the Bill pass in its current form.[16]

This system already exists in a scaled-down form in schools, where pupils and staff are surveilled. While the products used vary across schools, they can be as extensive as monitoring typing, file access and web search history, with this information collected, collated and retained by companies and in some cases interventions made. Encryption, rather than being broken in these systems, is just worked around. Anything, even bank details,[17] can be read or monitored on screen, regardless of whether the student is at school or not. The only thing that matters are the terms contained in the threat libraries.

For example, Impero's 'Education Pro' system[18] included the word "biscuit"[19] in their threat library on the grounds it is slang for guns. This system was used by more than "half a million students and staff in the UK" in 2018. "Taking a wonderful bath" is flagged on the grounds it is a reference to drugs.[20] There is little understanding or oversight over how these criteria are chosen or optimised. It is unclear who decides what does and does not trigger interventions across various school safety tech services. In December 2017 alone, eSafe claims they added 2,254 words to their threat libraries with no justification or explanation.[21] These systems

15 Scientific American, 'Apple's New Child Safety Technology Might Harm More Kids Than It Helps', August 2021: https://www.scientificamerican.com/article/apples-new-child-safety-technology-might-harm-more-kids-than-it-helps/

16 Politico, 'Liz '2 internets' Truss wants to change the online world', August 2022: https://www.politico.eu/article/liz-2-internets-truss-wants-to-change-the-online-world/

17 Smoothwall, 'Frequently Asked Questions': https://kb.smoothwall.com/hc/en-us/articles/360002135724-Frequently-Asked-Questions-FAQs-

18 The Guardian, 'Security flaw found in school internet monitoring software', July 2015: https://www.theguardian.com/technology/2015/jul/14/security-flaw-found-in-school-internet-monitoring-software

19 LinkedIn Pulse, 'Impero Software's Keyword Library for U.S. Schools Addresses Online Safety Concerns such as Self-harm and Radicalization', July 2016: https://www.linkedin.com/pulse/impero-softwares-keyword-library-us-schools-addresses-james-grew/

20 SecEd, 'Monitoring: Keeping up-to-speed', February 2019: https://www.sec-ed.co.uk/knowledge-bank/monitoring-keeping-up-to-speed/

21 John Colet School, 'Monitoring for Safeguarding Risks', 2018: https://www.johncolet.co.uk/assets/

are similar in design to those used by law enforcement to gather intelligence on terrorists and serious criminals. It is hard to understate the extent to which civil liberties would be harmed by scaling them up for application across an entire population using mainstream messaging services.

In the 2019 Online Harms White Paper,[22] the scope covers 'legal but harmful' activities and examples described as 'harms with a less clear definition' were nearly identical to terms used by school Safety Tech companies.[23] It is likely that one of the intended ends of the Bill is to facilitate the scaling up of safety tech companies. DCMS has recently undertaken analysis of the safety tech sector, projecting a compound annual growth rate of 35% per annum from 2021. Damian Collins MP, Minister for Tech and the Digital Economy praised the sector in a report, referring to it as a 'catalyst for UK growth', and going from 'strength to strength'.[24] At this point in time, it would appear to be the case that the Government intends to support the rapid growth of this sector, at the expense of privacy, security and multinational tech service providers operating in the UK.

A GLOBAL PRECEDENT

The UK has rightly criticised the Chinese Government over its surveillance of Hong Kong Chinese citizens, and has offered an extensive visa scheme to allow those fleeing growing CCP authoritarianism the opportunity to live and work in the UK. It is hypocritical to suggest that surveillance of encrypted messengers and private conversations should be permitted in the UK while it continues to maintain a stance against the same violations abroad. It would put the UK in the legislative company of Russia and China, countries that have totalitarian regimes the UK has made a strong point of standing against.

As the Government has stated, the Online Safety Bill is intended to be the first of its kind.[25] Countries across the world are looking to the UK's example to see the way it treats the right to privacy relative to its aim of increasing safety. It is effectively constructing a framework from which other countries pursuing similar ends can build on. If a lack of privacy and security is built into the OSB, the same could be the case when similar legislation is implemented in other countries, drastically undermining the right to privacy internationally.

Uploads/eSafe-Monitoring-for-Safeguarding-leaflet.pdf

22 DCMS and Home Office, 'Online Harms White Paper', April 2019: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf

23 Jen Persson's Blog, 'The Rise of Safety Tech', May 2021: https://jenpersson.com/the-rise-of-safety-tech/

24 DCMS and Perspective Economics, 'The UK Safety Tech Sector: 2022 Analysis', August 2022: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1095102/OS0057_UK_Safety_Tech_Analysis_2022_Online_v4__2_.pdf

25 DCMS, 'World-first online safety laws introduced in Parliament', March 2022: https://www.gov.uk/government/news/world-first-online-safety-laws-introduced-in-parliament

This could open up UK citizens' private communications to hostile action. The former Director of GCHQ has defended encryption as a necessity for greater societal privacy and safety, on the grounds that compromising the security and privacy of millions of people to gather intelligence on extremist groups and abusers is not proportionate.[26]

The UK Information Commissioner's Office (ICO) has also unequivocally endorsed end-to-end encryption[27]. Even Oliver Dowden MP, while he was the minister responsible for the Online Safety Bill, said:

> "If it was up to individuals within those companies to identify content on private channels, that would not be acceptable—that would be a clear breach of privacy."[28]

There is also strong consensus from technical experts on the need to protect privacy in the Bill. On 14th April 2022, 45 security experts and NGOs, including members of the Global Encryption Coalition signed an open letter, expressing concern that the accredited technology referenced in clause 103(2)(b) would require online service providers to compromise their own security, opening their users to hostile entities.[29] This wouldn't just be a blackmailer's charter—it would also present an opportunity for hostile governments to gather intelligence and undermine national security.

THE ECONOMIC THREAT FROM THE ONLINE SAFETY BILL

Compromising transatlantic trade of services

The OSB puts multinational tech companies in an untenable position.[30] Requiring a company to implement 'proactive technology' provides them with two options. Either to implement encryption backdoors or CSS software, compromising the security *and* privacy of their service, or simply stop operating in markets where this is required. For example, WhatsApp has not operated in China since being blocked

---

26 i News, 'Former GCHQ director Robert Hannigan: Encryption is a good thing', July 2017: https://inews.co.uk/news/technology/former-gchq-director-robert-hannigan-encryption-cannot-legislated-away-77837

27 Computer Weekly, 'ICO criticises government-backed campaign to delay end-to-end encryption' January 2021: https://www.computerweekly.com/news/252512294/ICO-criticises-government-backed-campaign-to-delay-end-to-end-encryption

28 Hansard, 'Online Harms Consultation, Volume 686', December 2020: https://hansard.parliament.uk/Commons/2020-12-15/debates/1B8FD703-21A5-4E85-B888-FFCC5705D456/OnlineHarmsConsultation#contribution-C6B532EC-E744-4084-BE3B-FBEB0386B354

29 Global Encryption Coalition, '45 organizations and cybersecurity experts sign open letter expressing concerns with UK's Online Safety Bill', April 2022: https://www.globalencryption.org/2022/04/45-organizations-and-cybersecurity-experts-sign-open-letter-expressing-concerns-with-uks-online-safety-bill/

30 The Economist, 'Britain's Online Safety Bill could change the face of the internet', May 2022: https://www.economist.com/britain/2022/05/25/britains-online-safety-bill-could-change-the-face-of-the-internet

by the Government in 2017. Last year, Signal was shut out of China.[31] While the motivations and censoriousness of the CCP are far more extreme than that of the Online Safety Bill, the end result could be similar. Cutting Britain out of using such products would not just undermine personal privacy. It would increase the friction of communication, making it harder for people to exchange information through popular, reliable services.

The alternative—staying in a market while trying to include weakened cryptographic features—has dire consequences. As recently as 1996 the UK withheld export licences from software companies, unless they implemented weak cryptography. To get around this, companies built support for different encryption algorithms for different markets, compromising the overall security of their products and enabling hostile actors to compromise software much more readily.[32]

Increased cost of business

Content moderation is costly. CSS systems are typically complemented by moderators, who make decisions on edge cases and help train the system to reduce its error rate. Facebook alone has already committed to allocating 5% of the firm's revenue, at $3.7 billion, on content moderation.[33] Adding further cost and complication for more extensive moderation in different markets could lessen the quality of services provided in the UK, undermine the Government's aim to encourage greater competition in digital markets[34] and encourage companies to develop and test new services in countries with less punitive regulatory regimes.

The UK represents roughly 2% of WhatsApp's customer base, and it has indicated it would choose to leave the market should it be required to implement content moderation or user profiling technology.[35] It is likely other companies offering similar services would choose to do the same if required to implement such technology.

Despite the size of the UK market, London is still the number one destination globally for US tech companies looking to expand, given its strong institutions, legal system and ease of business.[36] However, given concerns that the Bill could impose untenable requirements on such companies, it is possible large US companies would withdraw from the UK tech sector, which is currently valued at $1 trillion.[37]

---

31 South China Morning Post, 'China's Great Firewall ensnares encrypted messaging app Signal, joining Facebook's WhatsApp, Telegram among banned apps', March 2021: https://www.scmp.com/tech/policy/article/3125694/chinas-great-firewall-ensnares-encrypted-messaging-app-signal-joining

32 Wikipedia, 'Downgrade attack': https://en.wikipedia.org/wiki/Downgrade_attack

33 Knowledge at Wharton, 'How Social Media Firms Moderate Their Content', January 2022: https://knowledge.wharton.upenn.edu/article/social-media-firms-moderate-content/

34 DCMS, 'A new pro-competition regime for digital markets', May 2022: https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets

35 BBC News, 'WhatsApp: We won't lower security for any government', July 2022: https://www.bbc.co.uk/news/technology-62291328

36 London & Partners, 'London Looks to Strengthen Tech Trade and Investment Links With Us', May 2022: https://media.londonandpartners.com/news/london-looks-to-strengthen-tech-trade-and-investment-links-with-us

37 Silicon Republic, 'UK tech sector catches up with US and China at $1trn valuation': https://www.siliconrepublic.com/start-ups/uk-tech-sector-1-trillion-dollars-northern-ireland#:~:text=An%20analysis%20by%20Dealroom%20for,tech%20ecosystem%20at%20%241trn

If the UK is attempting to be an internationally competitive tech powerhouse, it could do a lot better than causing a flight of companies operating at that level. The US National Institute of Standards and Technology estimated that their advanced encryption standard, widely adopted online over the last 20 years, led to at least a $250 billion economic benefit.[38] Encryption and the privacy it protects builds trust in the digital economy, boosting consumer confidence and setting the foundation for advanced new products.[39] Undermining this confidence jeopardises one of our greatest sources of growth and innovation.

RECOMMENDATIONS

At the time of writing, DCMS' public position is to pass the OSB without significant amendment. To do so would have dire consequences for privacy, safety and security. While it is unlikely the Bill will be scrapped, its progress should be paused while Parliamentarians get to grips with its full implications. As such, DCMS should seek further evidence on the operation of and trade-offs required by the implementation of CSS systems.

In the absence of a fully rewriting the legislation, certain elements of the Bill should be removed entirely, including:

- **Clause 104(2)** which allows Ofcom to issue a notice requiring service providers to use 'accredited technology' to identify and 'deal with' content deemed harmful;
- **Clause 92(4)** which makes it an offence for the provider to give 'information which is encrypted such that it is not possible for Ofcom to understand it, or produces a document which is encrypted such that it is not possible for Ofcom to understand the information it contains';
- **Schedule 12** which further stipulates that failure to comply can lead to fines of up to £18 million or 10% of global revenue.

While far from an extensive set of recommendations, removing these clauses and schedules from the Bill is a first step towards protecting the right to privacy. At the very least, it is vital to ensure that the Secretary of State does not have broad, undefined powers to influence Ofcom's remit, thereby keeping politics out of the foundational structures of the internet. Schedule 12 also represents an extremely punitive condition for service providers' failure to comply with the abstract term of 'dealing with' harmful content, and is at odds with the UK's pro-competition regime for digital markets.[40]

---

38 National Institute of Standards and Technology, 'NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study', September 2018: https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

39 Niskanen Center, 'Encryption, Trust, and the Online Economy', November 2015: https://www.niskanencenter.org/wp-content/uploads/old_uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf

40 DCMS, 'A new pro-competition regime for digital markets', May 2022: https://www.gov.uk/government/consultations/a-new-pro-competition-regime-for-digital-markets

CONCLUSION

The Online Safety Bill represents an unprecedented threat to civil liberties. The Adam Smith Institute and others have already made a case against the 'legal but harmful' conditions threatening freedom of speech.[41] It also represents a fundamental threat to online privacy and security. The Bill, in broadening Ofcom's abstract criteria to issue notices to tech companies to 'deal with' harmful content will likely bring about a significant chilling effect not only to free expression online, but also creates untenable market conditions for tech services providers like encrypted messenger services. Individual privacy, security and the UK's competitiveness as a world class tech hub are all seriously threatened by the Bill passing in its current form.

---

41 Adam Smith Institute, 'Written evidence submitted by The Adam Smith Institute (OSB0129)': https://committees.parliament.uk/writtenevidence/39293/pdf/