Written evidence submitted by the Internet Society on the Online Safety Bill (OSB109)

1. The Internet Society welcomes the opportunity to comment on the Online Safety Bill. We would like to offer two documents highlighting our concerns with the Online Safety Bill's implications for end-to-end encryption and the Internet itself.

2. Founded in 1992, the Internet Society is a U.S. non-profit organization headquartered in Reston, Virginia and Geneva, Switzerland for the worldwide coordination of, and collaboration on, Internet issues, standards, and applications. As a global non-governmental organization, the Internet Society believes that the Internet is for everyone. It supports and promotes the development of the Internet as a global technical infrastructure, are source to enrich people's lives, and a force for good in society, with an overarching goal that the Internet be open, globally connected, secure, and trustworthy. The Internet Society's staff includes technical experts in internetworking, cybersecurity, and network operations, as well as policy experts in a broad range of Internet-related areas.

3. In 2020, the Internet Society co-founded the Global Encryption Coalition and is a member of the coalition's Steering Committee. With over 300 member organizations around the world, the Global Encryption Coalition promotes and defends encryption globally, focusing on key countries and multilateral fora where it is under threat.

4. On 24 November, the Internet Society joined nearly seventy civil society organizations, companies, legislators, and cybersecurity experts in an open letter [Annex 1] to Prime Minister Sunak expressing their concerns that the Online Safety Bill will undermine end-to-end encryption. As noted in the letter by the signers, many of them members of the Global Encryption Coalition, the Online Safety Bill would not only hurt the security and privacy of individuals but would also undermine trust in the British tech industry, limiting their ability to successfully compete in foreign markets or attract investment. Despite revisions to the Online Safety Bill, the legislation continues to pose a serious threat to the use of end-to-end encryption and the security and privacy the technology provides everyone.

5. In January 2022, the Internet Society released its Internet Impact Brief on the Online Safety Bill [Annex 2]. The Internet Impact Brief outlines the impact that the Bill's undermining of end-to-end encryption would have on the critical properties of the Internet. The Impact Brief found that if implemented, the Online Safety Bill "may negatively impact the Internet, pulling it away from its full potential as an open, globally connected, secure and trustworthy resource for all." Our fundamental conclusions remain unchanged by subsequent amendments to the Bill.

6. For economic security, a free society and the safest Internet possible for UK citizens, the Internet Society urges the Committee to ensure that the Online Safety Bill does not undermine end-to-end encryption.

Submitted by Robin Wilton, Director – Internet Trust, 12 December, 2022.

Annex 1: Open Letter to the Rt. Hon. Rishi Sunak MP, Prime Minister – November 2022

On 24 November, seventy civil society organizations, companies, elected officials, and cybersecurity experts, including Global Encryption Coalition members, published an open letter to British Prime Minister Rishi Sunak highlighting their concerns with the threat that the United Kingdom's Online Safety Bill poses to end-to-end encryption.

Dear Prime Minister Sunak,

With cyber attacks becoming ever-more frequent and sophisticated,[1] the reliance of UK citizens and businesses on end-to-end encryption to keep themselves safe and secure has never been greater.

Encryption is critical to ensuring Internet users are protected online, to building economic security through a pro-business UK economy that can weather the cost of living crisis, and to assuring national security. As you begin your new role as Prime Minister, the undersigned civil society organisations and companies, including members of the Global Encryption Coalition,[2] urge you and your government to ensure that encryption is not weakened.

Despite its intention to make the UK safer, the Online Safety Bill currently contains clauses that would erode end-to-end encryption in private messaging. As noted in a recent letter by leading UK digital rights organisations, the Bill poses serious threats to privacy and security in the UK "by creating a new power to compel online intermediaries to use 'accredited technologies' to conduct mass scanning and surveillance of all citizens on private messaging channels."[3] Leading cybersecurity experts have made clear that even message scanning, mistakenly cited as safe and effective by its proponents, actually "creates serious security and privacy risks for all society while the assistance it can provide for law enforcement is at best problematic."[4]

Undermining protections for end-to-end encryption would make UK businesses and individuals less safe online, including the very groups that the Online Safety Bill intends to protect. Furthermore, because the right to privacy and freedom of expression are intertwined, these proposals would undermine freedom of speech, a key characteristic of free societies that differentiate the UK from aggressors that use oppression and coercion to achieve their aims.

UK businesses are set to have less protection for their data flows than their counterparts in the United States or European Union, leaving them more susceptible to

cyber-attacks and intellectual property theft. UK digital businesses will also face new challenges in foreign markets. When Australia passed a similar law undermining end-to-end encryption in 2018, the Australian digital industry lost an estimated $AUS 1 billion in current and forecast sales and further losses in foreign investment as a result of decreased trust in their products.[5] As the UK economy faces significant challenges in the wake of COVID-19 and the impacts of the War in Ukraine, it is critical that the Bill does not undermine UK tech leadership and economic security.[6]

Undermining end-to-end encryption or introducing content scanning obligations for private messaging will also remove protections for private citizens' data. Opening a backdoor for scanning also opens a backdoor for cyber criminals intent on accessing our bank account details, private messages and even the pictures we share online privately with family and friends. We all deserve the protection that end-to-end encryption provides, but the most vulnerable in society – children and members of at-risk communities – need it most of all.

For economic security, a free society and the safest Internet possible for UK citizens, we call upon you and the UK government to ensure that the Online Safety Bill does not undermine end-to-end encryption.

Signatories*

Access Now

The Adam Smith Institute

Advocacy for Principled Action in Government

Aspiration

Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI)

Betapersei, S.C.

Big Brother Watch

Blacknight Internet Solutions Ltd

Jon Callas, Director of Public Interest Technology, EFF

L. Jean Camp, Professor, Indiana University

Center for Data Innovation

Center for Democracy and Technology

Center for New Liberalism

Centre for Policy Studies

CIPPIC (Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic)

Lord Tim Clement-Jones

Collaboration on International ICT Policy for East and Southern Africa

comun.al, Digital Resilience Lab

CRYPTO ID – BRAZIL

DNS Africa Media and Communications

Electric Coin Co. (creators and supporters of Zcash)

Electronic Frontier Foundation

Encrypt Uganda

Fight for the Future

Global Partners Digital

Markéta Gregorová, Member of the European Parliament

Index on Censorship

Dr. Philip Inglesant

Internet Freedom Foundation, India

Internet Society

Internet Society – Brazil Chapter

Internet Society Catalan Chapter

Internet Society Côte d'Ivoire Chapitre

Internet Society Colombia Chapter

Internet Society Ghana Chapter

Internet Society India Hyderabad Chapter

Internet Society Tanzania Chapter

Internet Society Tchad chapter

Internet Society Liberia Chapter

Internet Society Niger Chapter

Internet Society Portugal Chapter

Internet Society UK England Chapter

Interpeer gUG (haftungsbeschraenkt)

JCA-NET(Japan)

Kijiji Yeetu

C. de Larrinaga

Matthew Lesh, Head of Public Policy, Institute of Economic Affairs

Liberty

MEGA

Alec Muffett, Security Researcher

New America's Open Technology Institute

Numex

OpenMedia

Open Rights Group

Organization for Identity and Cultural Development

Ranking Digital Rights

People's Privacy Network

Chip Pitts

Sharon Polsky MAPP, President, Privacy & Access Council of Canada

Runa Sandvik, Founder, Granitt

Jamie Stone MP, Liberal Democrats

Superbloom

Surfshark

Susan Landau, Bridge Professor of Cyber Security and Policy, Tufts University

Tech for Good Asia

The Tor Project

Tutanota

TwelveDot Incorporated

University of Bosaso

Phil Zimmermann

*Affiliations listed for identification purposes only

[1] https://www.gov.uk/government/news/businesses-urged-to-boost-cyber-standards-as-new-data-reveals-nearly-a-third-of-firms-suffering-cyber-attacks-hit-every-week
[2] With over 300 members distributed across every region of the world, the Global Encryption Coalition promotes and defends encryption in key countries and multilateral fora where it is under threat. It also supports efforts by companies to offer encrypted services to their users. https://www.globalencryption.org/

[3] https://cloud.openrightsgroup.org/nextcloud/s/irGJD4GSRx3d4Mb

[4] https://arxiv.org/abs/2110.07450
[5] https://www.internetsociety.org/news/press-releases/2021/new-study-finds-australias-tola-law-poses-long-term-risks-to-australian-economy/
[6] https://www.gov.uk/government/news/uk-tech-sector-achieves-best-year-ever-as-success-feeds-cities-outside-london

Internet Impact Brief

End-to-end Encryption under the UK's draft Online Safety Bill

Internet Society , Callum Voge and Robin Wilton
Internet Society England Chapter

Version 1.0(January 2022)

Abstract

In May 2021 the UK published the draft Online Safety Bill (the "draft bill") which seeks to set out a new regulatory framework to protect Internet users from illegal and harmful content. If implemented in its current form, this draft bill may negatively impact the Internet, pulling it away from its full potential as an open, globally connected, secure and trustworthy resource for all.

This brief uses the Internet Impact Assessment Toolkit[1] (IIAT) to assess how the limitations placed on the use of end-to-end encryption under the UK's Online Safety Bill may affect the global Internet.

Context and Assumptions

Context

The UK published the draft Online Safety Bill on 12 May 2021. It is designed to establish a new regulatory framework to tackle harmful content online.[2] The draft bill was subject to a period of pre-legislative scrutiny by a Joint Committee of Members of the House of Commons and Peers from the House of Lords. This review concluded with a report published by the Joint Committee on 14 December 2021 detailing its recommendations.[3] The Government must now consider the findings of the Joint Committee's report and develop a new proposal on the Online Safety Bill before it can go to Parliament. It is expected that the Government will publish a revised proposal by March 2022.

The draft Online Safety Bill, like its predecessor the Online Harms White Paper,[4] would impose a statutory duty of care on certain service providers to moderate user-generated content so that users are not exposed to illegal and harmful online content.[5] Duty of care obligations differ based on the category that a service provider may fall into. These categories include: (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"; and (4) search engine providers.

The draft Bill grants the Office of Communications (Ofcom) the authority to oversee and enforce the new regime. In this role Ofcom will articulate codes of practice for the implementation of this duty of care for the four categories. The Draft Bill additionally suggests that the Secretary of State for the Department of Digital, Culture, Media and Sport (DCMS) will have the power to add or remove services from an exemption list and to set the thresholds that would place particular service providers into one of the four categories.

---

[1] https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/ The IIAT was developed by the Internet Society[1] to be used by anyone who wants to check if a particular policy, development, or trend affects the critical properties of the Internet Way of Networking (IWN).

[2] https://www.gov.uk/government/publications/draft-online-safety-bill

[3] https://publications.parliament.uk/pa/jt5802/jtselect/jtonlinesafety/129/12902.htm

[4] https://www.gov.uk/government/consultations/online-harms-white-paper

[5] https://www.lawfareblog.com/uks-online-safety-bill-not-safe-after-all

Ofcom can require that service providers use "accredited technology" to identify harmful content and "swiftly take down that content". To comply with this requirement and fulfil their "duty of care", service providers will likely need to resort to upload filters and other mechanisms that may interfere with the use of end-to-end encryption.[6]

How is encryption implicated in the Draft Online Safety Bill?

Encryption is a data confidentiality mechanism designed to help Internet users keep their online data and communications private and secure. It plays a critical role in protecting day-to-day digital activities like online banking, shopping, preventing theft of sensitive information in data breaches, and making sure private messages stay private.

Encrypted messaging works by scrambling information so that it can only be read by someone with the "key" to open and unscramble the information. End-to-end encryption provides the strongest level of security and trust, as only the intended recipients hold the key to decrypt the message. In end-to-end encryption, no third party — including the service provider or the government — can read users' encrypted content. End-to-end encryption is used in daily life including for personal messaging, video conferencing, online shopping, and banking transactions.[7]

The draft Online Safety Bill places a duty of care on service providers within the scope of the draft bill to moderate illegal and harmful content on their platforms, with fines and penalties for those that fail to uphold this duty. The only way for service providers that offer end-to-end encryption to comply with this duty of care would be to remove or weaken the encryption that they offer. In this sense, while the text of the Online Safety Bill does not explicitly ban end-to-end encryption, the liabilities it imposes on service providers would create strong incentives for providers to withdraw end-to-end encrypted services from the market. Doing so would enable service providers to intercept users' communications to avoid violating the duty of care placed on them. The report published by the Joint Committee on 14 December 2021 asked the Government to clarify how the providers of encrypted services should comply with the duty of care ahead of the draft bill being introduced into Parliament. The report additionally recommended that end-to-end encryption be included in risk profiles and risk assessments, requiring providers to identify and address these risks.

Related activities separate to the Online Safety Bill

On 29 June 2021 DCMS published guidance titled: Public and private channels: improve the safety of your online platform.[8] This guidance, while separate from the Online Safety Bill, provides insight into Government thinking behind the duty of care. For example, the guidance states that end-to-end encryption makes it more difficult to identify illegal and harmful content on private channels and recommends removing end-to-end encryption for children's accounts.

[6] https://www.openrightsgroup.org/blog/encryption-in-the-online-safety-bill/

[7] https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/

[8] https://www.gov.uk/guidance/private-and-public-channels-improve-the-safety-of-your-online-platform

This DCMS guidance contradicts the UK's 2020 Age appropriate design code which aims to minimize the collection of children's data.[9] The code encourages providers to conduct data protection impact assessments to mitigate risks to the rights and freedoms of children, pointing to encryption as a technological security measure.[10] The contradiction arises in that DCMS guidance asks that providers increase their collection of children's data for their 'safety' while the Age appropriate design code recommends the exact opposite, also in the name of safety.

Additionally, in September 2021 the Home Office launched a new Safety Tech Challenge Fund, which awarded five organizations up to £85,000 each to develop "innovative technologies" for law enforcement access to online messaging platforms with end-to-end encryption.[11]

Over 90 civil society organizations[12] have criticised Apple's August 2021 proposed use of client-side scanning for its potential for abuse and the risks it poses to certain youth groups, including LGBTQ youths. Recognizing these concerns, Apple has since scrapped its planned changes to messaging for youth accounts. Despite this, in the Daily Telegraph article announcing the Safety Challenge Fund, Home Secretary Priti Patel pointed to Apple's client-side scanning proposal as a positive example, raising concerns about the criteria for evaluating Challenge Fund proposals.[13]

Together, the text of the Draft Online Safety Bill and the governments accompanying communication campaign implies a wider intention to drive end-to-end encryption from the UK market.

Assumption: Exclusion of Internet Infrastructure

Based on the text of the Online Safety Bill, this brief assumes that consumer services that allow for user-generated content such as Signal, WhatsApp, iMessage, and Zoom would be the providers most likely to face pressures to weaken encryption under the duty of care.

The Internet Society's understanding is that Internet infrastructure providers, such as Internet Service Providers (ISPs), will remain out of the scope of the Draft Online Safety Bill and that the 2016 Investigatory Powers Act[14] will continue to regulate them.

For this reason, we have limited our analysis to the Draft Bill's impact on consumer-facing services, primarily messaging and video conferencing. We do, however, acknowledge the danger of scope creep and the potential that pressure to weaken encryption could spread to Internet infrastructure providers in the future.

[9] https://techcrunch.com/2021/09/01/uk-now-expects-compliance-with-its-child-privacy-design-code/

[10] https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-onlineservices/2-data-protection-impact-assessments/

[11] https://homeofficemedia.blog.gov.uk/2021/09/08/new-safety-tech-fund-challenge/

[12] https://cdt.org/insights/international-coalition-calls-on-apple-to-abandon-plan-to-build-surveillance-capabilities-into-iphones-ipads-andother-products/

[13] https://www.telegraph.co.uk/politics/2021/09/08/priti-patel-call-worlds-tech-giants-please-dont-put-profit-safety/ [14] https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

Definition of Weak Encryption

This paper references the weakening of strong encryption either through its removal for certain demographics (for example, children) or through the creation of "encryption backdoors".

Certain policymakers and law enforcement agents in the UK suggest that the Draft Online Safety Bill will not necessitate the removal of end-to-end encryption in entirety and instead would just require "exceptional access"[14] for law enforcement agencies through the use of "encryption backdoors".[15]

This assessment is inaccurate from a technical standpoint as end-to-end encryption with backdoors is not true end-to-end encryption. [16] The definition of end-to-end encryption is that no third party, including the service provider or government authorities, holds the key to decrypt messages sent through this method. The process of encryption occurs on a user's personal device before being transmitted to the recipient's device, where only then the process of decrypting begins.

The consensus among technical experts is that there are currently no technical solutions that would allow only certain actors access to private communications and not others.[17] The creation of a backdoor for law enforcement access also creates a common gateway that criminals and hostile state actors can use.

Given the above considerations, this brief considers both the removal of encryption for certain groups and the creation of backdoors as a weakening of encryption.

[14] https://www.theguardian.com/uk-news/2020/feb/25/mi5-chief-asks-tech-firms-for-exceptional-access-to-encrypted-messages

[15] https://www.computerweekly.com/news/252447999/UK-and-allies-call-for-backdoors-in-encryption-products

[16] https://academic.oup.com/cybersecurity/article/1/1/69/2367066

[17] https://www.globalencryption.org/2020/11/breaking-encryption-myths/

How does the Online Safety Bill Affect the Full Potential of the Internet?

The Internet rests upon several unique foundational properties that have facilitated its growth and fuelled innovation for communities around the world. Yet to achieve the Internet's full potential it is necessary to look beyond this foundation to the mechanisms that enable an Internet that is an open, globally connected, secure and trustworthy resource for everyone. The following section analyses how the Draft Online Safety Bill may prevent the Internet from reaching its potential, by considering each of the enabling factors in turn.

Easy and unrestricted access

It is easy to become part of the Internet, for networks and users alike. Networks operators can easily add themselves to the Internet's infrastructure without unnecessary regulatory or commercial barriers. Responsive Internet infrastructure creates an Internet that is affordable for users and that has accessible services, empowering users to connect and use the Internet with minimal barriers.

If the draft Online Safety Bill is implemented in its current form, providers will face the impossible task of creating encryption backdoors that are secure. The creation and management of such backdoors would be a costly process. Besides the initial cost of the backdoor's design, providers would likely need to have encryption engineers on constant standby to respond to attacks that will occur due to the vulnerabilities created by the backdoor.

Only the largest service providers will be able to afford these costs, leaving others even less secure. New players, including innovative UK start-ups, will likely lack the resources needed to enter the market, placing the UK's digital sector at a disadvantage, and hurting the UK's ability to compete globally.

These regulatory requirements and their accompanying costs adds a barrier to entry and will result in a less-open Internet with fewer service providers. This in turn will hurt user access, as options for connecting and using the Internet diminish.

Unrestricted use and deployment of Internet technologies

The Internet's technologies and standards are available for adoption without restriction. This enabler extends to end-points: the technologies used to connect to and use the Internet do not require permission from a third party, OS vendor, or network provider. The Internet's infrastructure is available as a resource to anyone who wishes to use it in a responsible and equitable way. Existing technologies can be mixed in and used to create new products and services that extend the Internet's capabilities.

The Online Safety Bill will limit how innovators can mix end-to-end encryption with new or existing technologies to create new products and services to the benefit of Internet users, hurting the UK's ability to lead in innovative digital services. The Online Safety Bill would create a barrier to adopting future cryptographic protocols that developers create to respond to ever-changing cybersecurity threats. As the rest of the world moves on to new technologies, UK service providers may lag behind with old technologies that are no longer fit for purpose.

The Draft Bill additionally grants Ofcom the power to serve technology notices to service providers that are noncompliant with their duty of care. These technology notices require the

provider to use “accredited technologies” to identify and remove public terrorism and Child Sexual Exploitation and Abuse content.[18]

References to “accredited technologies” place a limitation on the tools that service providers can use to stay compliant with Ofcom’s technology notices. This limits innovation and the ability of service providers to maximize efficiency and accuracy when pairing technologies to the specific task that they wish to complete. The accreditation of technologies also has ripple effects into other sectors, as providers in other industries that have not received technology notices will likely still opt to use accredited technologies out of an abundance of caution to ensure that they would be able to comply at a future date if needed.

Obligations under the draft Online Safety Bill’s duty of care restrict the use and deployment of current and future encryption technologies and standards, resulting in an Internet that is less open.

Unrestricted reachability

Internet users have access to all resources and technologies made available on the Internet and are able to make resources available themselves, contributing to the Internet’s role as a resource of global knowledge production. Once a resource has been made available in some way by its owner, there is no blocking of use and access to that resource by third parties.

Internet users who are no longer able to use end-to-end encryption technologies will find themselves excluded from resources and services made available on the Internet. Global consumer service providers may leave the UK market to ensure that they are outside the scope of the draft bill. UK Internet users that seek to share and access resources on these services will find themselves excluded, isolating UK Internet users from global knowledge production.

Likewise, individual Internet users may be wary of sharing resources on the Internet if they lack the security reassurances offered by encryption, reducing the flow of information and the resulting opportunities for collaboration, innovation, and business exchange.

By limiting end-to-end encryption technologies, the Draft Online Safety Bill will distort individual behaviour as well as the behaviour of global service providers, resulting in a less globally connected Internet.

Data confidentiality of information, devices, and applications

Data confidentiality, usually accomplished with tools such as encryption, allows end users to send sensitive information across the Internet so that eavesdroppers and attackers cannot see the content or know who is communicating. Allowing the transfer of sensitive information helps create a secure Internet. Data confidentiality also extends to data-at-rest in applications. (N.B., “confidentiality” also contributes to privacy, which is part of a trustworthy Internet).

End-to-end encryption is a tool that is used to ensure that sensitive information and communications are confidential between senders and receivers. Pressure from the Online Safety

[18] Chapter 4, Item 64.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookm arked.pdf

Bill to remove or weaken encryption through encryption backdoors will place UK businesses and individuals in danger.

For businesses, encryption protects transaction data and confidential business information from interception. End-to-end consumer messaging applications are used throughout the international business world, to negotiate partnerships and carry out exchanges. Research has shown that laws that weaken encryption fuel business uncertainty and can result in significant economic harm.[19]

Due to practical and financial motivations, providers that fall outside the scope of the draft bill will likely use the same encryption protocols used by those that fall within the draft bill, resulting in the widespread presence of encryption backdoors beyond messaging platforms. Given this incentive to use existing encryption algorithms and protocols across industries, policymakers will face the challenge of ensuring the use of strong encryption in certain contexts and the use of weakened encryption in other contexts.

The implementation of the draft bill may also shape developers' expectations, by motivating developers to design encryption algorithms that they can easily weaken to comply with the Online Safety Bill. Third parties could infiltrate sensitive information through backdoors to amass data on service providers outside the scope of the draft bill.

Flawed implementation has unintended consequences. For example, Juniper Networks, a tech giant that produces networking equipment for corporate and government systems, illustrates how the flawed implementation of encryption weaknesses intended for one industry can spill over into others.

In 2015 Juniper Networks announced that it had discovered an unauthorised backdoor that for at least three years had allowed third parties to decrypt data passing through its systems. Technical experts believe that this unauthorised backdoor occurred due to the use of a software component called Dual_EC, which had allegedly been re-engineered to grant the US National Security Agency "exceptional access" to decrypted data. The weaknesses in this component were then exploited by an unknown third party, believed to have been a hostile state actor, who capitalised on these weaknesses to create an unauthorised backdoor.[20] The presence of this unauthorised backdoor allowed the third party to intercept and manipulate sensitive information as it passed through government systems.

Examples like these highlight the spill over effects when encryption protocols and algorithms cross industries, mirroring the weaknesses intended for private messaging channels and placing critical infrastructure or even government systems in jeopardy.

Individuals also rely on encryption for confidentiality to ensure that what they choose to keep private in their physical lives also stays private in their online lives. There are unique concerns for vulnerable communities that rely on encryption to protect themselves from violence and discrimination. This includes the LGBTQ community,[21] domestic abuse survivors, and minority

[19] https://www.internetsociety.org/resources/doc/2021/the-economic-impact-of-laws-that-weaken-encryption/

[20] https://www.wired.com/2015/12/researchers-solve-the-juniper-mystery-and-they-say-its-partially-the-nsas-fault/

[21] https://www.internetsociety.org/wp-content/uploads/2019/11/Encryption-LGBT-Perspective-Fact-Sheet-EN.pdf

groups. Given the documented rise in LGBTQ-related hate crimes in the UK, this should be of concern to Her Majesty's Government.[22]

Civil servants, advocacy groups[24] and certain professions including journalists[23] and doctors additionally rely on encryption to do their jobs. While the draft Bill may attempt to carve out exemptions for certain groups, in practicality such exemptions will be difficult to maintain as communication between groups and with the public will occur across potentially incompatible encryption systems.

By limiting end-to-end encryption, the Online Safety Bill will reduce data confidentiality for UK businesses and individuals, harming Internet security.

Integrity of information, applications, and services

> Strong encryption helps ensure that the integrity of data sent over the Internet, and stored in applications, is not compromised. Critical underlying Internet services, such as DNS and the routing system, cannot be manipulated or compromised by malicious actors. Data stored in applications cannot be manipulated or compromised by third parties.

The Online Safety Bill pushes digital providers to either create encryption backdoors or remove end-to-end encryption. Encryption backdoors create new vulnerabilities that criminals or hostile state actors can exploit to access and potentially manipulate sensitive information.[13] There are currently no technical solutions to create gateways for law enforcement use without also making entry easier for third parties.[14]

The removal of end-to-end encryption in the UK will place the integrity of information at extreme risk. This will leave UK businesses and individuals vulnerable to malicious attacks that would compromise data.

UK businesses rely on end-to-end encryption to protect trade secrets and sensitive financial data.

Consumer messaging products are the de facto platforms for conducting business around the world. Attacks on decrypted information could see business records manipulated in efforts to harm the company's reputation, production capacity, or commit fraud. For example, in December 2021, hackers diverted a $130 million business transaction to a Hong Kong bank account by manipulating data in transit.[24]

Businesses outside the scope of the Draft Bill are likely to use the same encryption protocols, complete with backdoors, that businesses within the scope of the Draft Bill use due to practical and financial concerns related to adopting new technologies. Given the technical difficulty of designing encryption systems, engineers are motivated to avoid the duplication of efforts and build upon existing encryption protocols.

Mandating different encryption standards for different industries creates systemic complexities. In practice, developers embed encryption into products and services at various points in the

---

[22] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/839172/hate-crime-1819-hosb2419.pdf [24] https://www.internetsociety.org/resources/doc/2021/factsheet-how-encryption-can-protect-advocacy-groups-and-social-changemovements/

[23] https://www.internetsociety.org/wp-content/uploads/2020/03/Encryption-for-Journalists-Factsheet.pdf

[24] https://www.law360.com/cybersecurity-privacy/articles/1447476/chancery-probes-contract-risks-in-130m-merger-hack?nl_pk=8f274be7-bce7-4f2d-929a-36043970098f&utm_source=newsletter&utm_medium=email&utm_campaign=cybersecurity-privacy

supply chain, and often not at the final stage before consumer use. The complexity of enforcing different encryption standards along the supply chain could result in increased risk for consumers if data integrity is left unprotected.

The manipulation of this data could result in real world harm when hostile actors tamper with connected objects. For example, in July 2015 attackers exposed a vulnerability in the Uconnect system used by Chrysler vehicles by demonstrating their ability to remotely cut out the car's transmission and brakes as well as commandeer the steering wheel.[25] Unexpected encryption weaknesses in the supply chain of connected products would increase exposure to such attacks. Machine in the Middle (MITM) attacks may also become more common. These attacks occur when an individual secretly places themselves in the middle of a conversation, intercepting messages and either reading or altering them before passing them along. Without encryption, there is less assurance that the individual that you think you are communicating with is indeed who they say they are, opening individuals up to new scams and fraud.

In summary, the Draft Online Safety Bill's efforts to weaken encryption will reduce the integrity of data sent over the Internet and reduce Internet security, resulting in harm to businesses and individuals.

Reliability, resilience, and availability

The Internet is reliable when technology and processes are in place that permit the delivery of services as promised. If, for example, an Internet service's availability is unpredictable, then users will observe this as unreliable. This can reduce trust not just in one single service, but in the Internet itself. Resilience is related to reliability: a resilient Internet maintains an acceptable level of service even in the face of errors, malicious behaviour, and other challenges to its normal operations.

Users that communicate over encrypted services have the expectation that their communications are private and anonymised. The Draft Online Safety Bill's requirement to either remove or weaken encryption would result in private messages sent through so-called re-engineered encryption being read by law enforcement authorities as well as malicious actors who act to exploit the new vulnerabilities in the system.

The disconnect between what the users of encrypted services expect and what is delivered because of the Online Safety Bill will erode the public's perception of encryption's reliability. As perceptions deteriorate, the use of the Internet will likely also deteriorate.

For example, journalists may struggle to use the Internet to connect with sources if they cannot guarantee that their testimonials will remain confidential. Likewise, vulnerable communities such as LGBTQ youth may choose not to use essential services like suicide hotlines out of fear that their identity may be exposed, outing them, and putting them at risk of discrimination or violence. Such changes will hurt society, limiting our ability to hold power to account and further isolating vulnerable individuals.

[25] https://www.theverge.com/2015/7/21/9009213/chrysler-uconnect-vulnerability-car-hijack

When ‘re-engineered encryption’ under the Draft Online Safety Bill fails to deliver, public trust in encryption and the wider Internet will decrease, depriving the UK public of the Internet’s many benefits.

Accountability

Accountability on the Internet gives users the assurance that organizations and institutions they interact with are directly or indirectly acting in a transparent and fair way. In an accountable Internet, entities, services, and information can be identified and the organizations involved will be held responsible for their actions.

The Online Safety Bill grants regulatory powers to Ofcom to require that service providers within the scope of the draft bill to decrypt communications and make them available for law enforcement purposes. The draft of the bill does not set thresholds for the type or volume of data shared in these circumstances. It also does not provide a mechanism for users to track when and how their data is shared. Without further clarification, Internet users will lack the assurance that their private data is used appropriately.

The Draft Bill additionally grants the Secretary of State for Digital, Culture, Media and Sport with the power to add or remove providers from an exemption list based on the risk of harm to individuals. The Draft Bill does not set clear limitations on this power, allowing for a high degree of discretion, and creating openings for misuse.

The Draft Bill does not provide guidance on the distinction between content that is “illegal” and content that is “legal but harmful” despite both categories being within the scope of the Draft Bill. Ofcom’s forthcoming codes of practice will define the types of content that will be moderated and set concrete expectations for service provider behaviour under the four levels in the duty of care. These codes of practice must clarify how data in private messages, particularly encrypted private messages, is treated differently from publicly posted data. This would include the threshold needed to grant law enforcement access, limitations on the storage and transferring of private data, and mechanisms for users to report undue censorship, among others.

It is important to acknowledge that the draft bill provides special protections for journalistic content and “content of democratic importance”. The inclusion of such limitations increases accountability. However, the ambiguous definitions of these protections only give a semblance of accountability. For example, an Internet user may be unsure if the content they produce is of democratic importance, or not.

Without proper accountability functions that place limitations on data requests and exemption lists, the Online Safety Bill threatens to reduce accountability on the Internet, decreasing its trustworthiness.

Privacy

Privacy on the Internet is the ability of individuals and groups to understand what information about them is being collected and how, and to control how this is used and shared. Privacy often includes anonymity.

End-to-end encryption provides users with the ability to communicate freely with the assurance that only their intended recipient will be able to access and use their data. By effectively removing

end-to-end encryption, the Draft Online Safety Bill reduces these privacy assurances, reducing the ability of Internet users to control the movement of their data and creating uncertainty as to who can access, share, and store their data.

The right to privacy is closely related to freedom of expression. Individuals may self-censor their private communications due to anxiety of their personal data being abused in a phenomenon called the chilling effect. Without guarantees and transparency as to how data is collected, used, and stored individuals will fear that the things they keep private in their real lives will not remain private in the digital lives. Meanwhile, businesses may fear that their trade secrets, commercial and financial communications, and privileged communications are inappropriately accessed and shared.

Strict guidelines for government use, storage, and access to data is essential for protecting privacy. Yet, even governments with the most stringent data laws will be unable to protect private data from criminals and third parties when encryption is weakened. These privacy violations will be particularly concerning to UK national security if hostile state actors are able to discreetly collect and process the data of high-profile individuals. Privacy violations may lead to related political consequences, such as the revoking of the June 2021 data adequacy decision granted to the UK by the EU.[26]

Loss of privacy may also have ramifications for the safety of children when their private data is no longer protected and may more easily by exploited by predators to obtain sensitive images or for grooming purposes – directly countering one of the main objectives of the Draft Bill.

Even in countries like the UK where rule of law is strong, government or law enforcement access to private communications could be abused by individuals that violate the agreed norms and use their privileged access to track political dissent or utilize private data for personal gain.

A further consideration is needed for the precedent that the Online Safety Bill will set for the rest of the world. By implementing regulation that places holds on the use of end-to-end encryption the UK will empower other countries with potentially less robust rule of law standards to enact similar legislation. In these scenarios government abuse of private data may be used in a systemic manner to further authoritarian goals with no checks and balances. This not only may be harmful to the UK's reputation as a defender of human rights but may also exacerbate geopolitical issues as other states consolidate control over the information and resources that their citizens have access to.

The Online Safety Bill's weakening of encryption presents serious privacy concerns with consequences for individuals, businesses, and national security. The global precedent that the Online Safety Bill sets may empower authoritarian governments around the world to systematically crack down on privacy, cementing their control over information and harming the UK's reputation as a defender of human rights.

[26] https://ec.europa.eu/commission/presscorner/detail/ro/ip_21_3183

Summary & Recommendations

Using the Internet Impact Assessment Toolkit, this brief has found that encryption requirements under the UK's Draft Online Safety Bill will negatively impact all four of the qualities that maximize the Internet's potential as a resource for good: open, globally connected, secure and trustworthy.

By infringing upon easy and unrestricted access to the Internet as well as the unrestricted use and deployment of Internet technologies, the Draft Online Safety Bill will make the Internet a less open resource while by reducing the Internet's reachability it will limit global connectivity. The Draft Online Safety Bill likewise harms Internet security by reducing the confidentiality and integrity of information passing through its system. Internet trustworthiness is also reduced under the Draft Online Safety Bill as privacy guarantees are lost, accountability weakened, and reliability, resilience, and availability reduced.

These losses will have important consequences for UK businesses, Internet users, and vulnerable communities as well as the global reputation of the UK. The duty of care articulated in the draft Bill focuses on the duty of providers to protect users from exposure to harmful content but fails to address the duty of providers to equip users with the tools to protect themselves online.

In this sense, while the Draft Online Safety Bill claims that it will make the UK 'the safest place in the world to be online,' this report has found that by dismantling strong encryption, the Bill will confront UK Internet users with an Internet that is more insecure and unsafe than before.

This brief offers three recommendations:

1. That the Draft Online Safety Bill be redrafted so that it is compatible with strong, end-to-end encryption. Encryption is an essential element of an open, globally connected, secure and trustworthy Internet.
2. That removing or weakening encryption through backdoors be actively discouraged due to the accompanying security risks. There are currently no technical solutions that would grant law enforcement access to encrypted messages without also creating vulnerabilities that could be exploited by malicious third parties.
3. Finally, it is recommended that a full and robust Internet impact assessment is conducted by Her Majesty's Government to identify the potential harms to the Internet resulting from weakened encryption under the Draft Online Safety Bill. This Assessment should build upon the existing Impact Assessment, which failed to adequately examine encryption and inter-related issues. The Assessment should also be conducted at an early date, to ensure that Parliament is fully informed during the legislative process.