BREAKING ENCRYPTION IS LEGALLY & PRACTICALLY UNWORKABLE

LEGAL REPORT

INDEX ON CENSORSHIP
A VOICE FOR THE PERSECUTED

Executive Summary

Breaking encryption is legally & practically unworkable

This report builds upon years of work by Index on Censorship, parliamentarians, and independent counsel at Matrix Chambers to clearly and unequivocally demonstrate that "Technology Notices" (as defined below) that can be issued by Ofcom under s. 121 of the Online Safety Act 2023 (the "**OSA**") are fundamentally incompatible with international and domestic human rights laws: their effect would amount to ending access to end-to-end encrypted messaging in the United Kingdom, contravening Articles 8 and 10 of the European Court of Human Rights and breaching Ofcom's obligations under the Human Rights Act 1998, fundamentally alter the face of digital communications in the United Kingdom, and leave the UK government vulnerable to a barrage of diplomatic and international legal disputes.

At Index on Censorship, we have published censored writers across the globe since 1972. Today, we're using encrypted messaging apps to keep in touch with our network of correspondents around the world, from Iran, to Afghanistan, to Hong Kong.

We were vindicated in raising the alarm over the government's ongoing crusade against encryption, its potential abuse under the IPA, and we have repeatedly called for Ofcom's power to issue Technology Notices to be removed from the OSA given their legal and practical failings.[1]

While the OSA's aims are commendable, the road to mass censorship is paved with good intentions, and the Government still has the chance to avoid this legal headache and practical international embarrassment.

[1] *Index on Censorship: Online Safety, or Surveillance*

If you would like more information and to discuss encryption with the experts, please contact indexencryption@89up.org

What is End-to-end Encryption?

Major Service Providers such as Whatsapp - who alone services 42m users in the UK[2] - Telegram, and Signal, use E2EE, allowing their users to securely send private messages that only they can read. E2EE works by scrambling the contents of a message into unintelligible code using a pair of cryptographic keys. In systems protected by E2EE, only the sender and the recipient hold the keys needed to decrypt the message, meaning that no one else - not even the Service Provider itself - can access its contents.

E2EE is an essential factor in protecting individuals and businesses from hacking, identity and personal data theft, and fraud, and it is a critical tool used by individuals for whom their safety and security depend on their communications being private and secure. This includes journalists communicating with their sources, dissidents under authoritarian regimes, human rights defenders, and victims in victim support groups.

What are 'Technology Notices' in the Online Safety Act?

S.121 OSA allows Ofcom to issue notices ("**Technology Notices**") to user-to-user services or regulated search services ("**Service Providers**"), requiring them to identify and take down terrorism content and child sexual exploitation and abuse content from their services.

S.121 OSA mandates that this be done by the use of "accredited technology" - technology which the Government has admitted does not yet exist, but which is likely to be a form of client-side scanning ("**CSS**"). CSS is a technology that scans messages on a user device before they are sent, checking them against a database of offending content. If a message is flagged as a match against the database, it would then need to undergo further review to decide whether it should be taken down.

As soon as the first Technology Notice is issued under the Online Safety Act as the text stands - two scenarios become available - both of which fundamentally undermine end-to-end encryption in the UK and breach UK citizens' human rights under Articles 8 and 10 of the ECHR.

[2] *Backlinko, "WhatsApp User Statistics 2025: How Many People Use WhatsApp?," Backlinko, last modified August 18, 2025, https://backlinko.com/whatsapp-users.*

If you would like more information and to discuss encryption with the experts, please contact indexencryption@89up.org

The legal implications
Of breaking end-to-end encryption

As will be discussed at length in this report, the practical challenges with, and burden of, implementing CSS would likely lead to the complete removal of E2EE in the UK by Service Providers withdrawing their services in the UK, or electing to remove end-to-end encryption ("**E2EE**") as an option on the UK parts of their services. However, a closer look at the two possible scenarios (the complete removal of E2EE in the UK, or the introduction of CSS) show that both fundamentally undermine E2EE in the UK and are incompatible with international human rights laws.

Scenario 1: Complete removal of E2EE in the UK

As flagged by Matthew Ryder KC in his legal opinion, Technology Notices would not have their intended effect if they were issued to only one Service Provider. If only one Service Provider in the UK scanned for and took down offending content, people sending such offending content or communications would simply switch to another messaging service. As such, the likely scenario is that Ofcom would issue Technology Notices to all Service Providers in the UK simultaneously.

The prospect of all such Service Providers electing to end E2EE on the UK parts of their services, leading to a complete removal of E2EE in the UK, is not a theoretical threat; Apple recently removed end-to-encryption as an option for its UK users on some of its iCloud data categories after being served with a "technical capability notice" by the Home Office under the Investigatory Powers Act 2016 (the "**IPA**"), requesting access to customer data. In response, Apple launched a legal challenge against the Home Office, the proceedings of which are still ongoing. The Home Office is believed to have withdrawn from its defence, but has instead issued a new notice relating to data of British subjects only. Further, WhatsApp has said that they will leave the UK (which constitutes 2% of its global customer base) rather than comply with the requirements of a Technology Notice.

If this happens, the UK would be leading the way as one of the first democracies to place a *de facto* ban on E2EE for private messaging apps. Measures which have the effect of weakening encryption also contravene established ECHR law, as first considered in the case of *Podchasov v Russia App No. 33696/19 ("Podchasov")*.

Scenario 2: Introduction of Client-side Scanning

However, even if Service Providers chose not to remove their E2EE services from the UK, the implementation of CSS would constitute mass surveillance of private communications of UK citizens. The prospect of every Service Provider user having their private messages scanned before they are sent, and potentially undergoing further human review, is a previously unimaginable, dystopian prospect. It would also erode user privacy, and literature shows that introducing CSS weakens the security of E2EE systems - again, something that is likely to contravene ECHR law under the *Podchasov* case.

Matthew Ryder KC highlights in his legal opinion that the mass surveillance mandated under s. 121 OSA carries significant similarities with "bulk surveillance". The execution of bulk surveillance requires certain safeguards established by ECHR law to protect individuals' Article 8 and Article 10 rights. As will be shown in this report, the OSA is wholly insufficient with respect to meeting such safeguards. Additionally, surveillance which may uncover journalistic materials and sources, and hamper journalistic freedom of expression, carries with it even stricter requirements in order to be legal - something which the OSA also insufficiently fails to address.

The Government already has certain surveillance powers under the IPA. Crucially, such surveillance can only be carried out by intelligence services. The use by Ofcom of Technology Notices would constitute an obscene expansion of pre-existing surveillance powers, without the strict safeguards contained in the IPA (or as required by ECHR law), and mandate private technology companies to carry out such surveillance on behalf of the state. By definition, no communications in the UK would be private. As Matthew Ryder KC found:

> *"Ofcom will have a wider remit on mass surveillance powers of UK citizens than the UK's spy agencies, such as GCHQ (...) Section 104 [now s. 121] notices amount to state-mandated surveillance because they install the right to impose technologies that would intercept and scan private communications on a mass scale."*[3]

This would constitute some of the broadest and most powerful surveillance powers ever proposed in any Western democracy - putting Britain practically closer in line with North Korea and Russia with how it treats citizens' communications.

The obligation to comply with and protect ECHR rights extends to public authorities in the UK, which includes Ofcom. Where public authorities compel private actors to take steps which may interfere with or violate ECHR rights, such interferences may be attributable to

[3] *https://www.indexoncensorship.org/2022/11/new-legal-opinion-on-the-online-safety-bill/*

the relevant public authority or state. Any attempts to remove E2EE or implement CSS by Service Providers may be brought against the UK state under ECHR law.

For state interferences with ECHR rights to be legal, their effects must be proportionate to the aims pursued (i.e., they must meet what is called the "principle of proportionality"), and they must meet the "principle of legality". Given the extreme impact that the use of Technology Notices would have on users' privacy and freedom of expression, as shown in the legal opinions commissioned by Index on Censorship, it is unlikely that the removal of E2EE, or the weakening of E2EE systems by the introduction of CSS, by the use of Technology Notices will be proportionate to the aims of s. 121 OSA. Further, the vague nature of the legislation means it is unlikely to meet the principle of legality. As such, it is our contention that Ofcom's powers under s. 121 OSA are illegal under ECHR law.

However, this is by far not the only critical issue with the legislation. As set out in this report, other areas of concern include the following:

Whether Service Providers elect to remove/break encryption in the UK or use CSS, the outcome is the same: contravention of UK citizens' human rights. In either scenario, once a Technology Notice has been issued it will have contravened UK citizen's human rights under Articles 8 and 10 of the ECHR, for which the UK government will be liable. This, even before contemplating the severe practical issues and consequences of breaking end-to-end encryption.

The practical implications
Of breaking end-to-end encryption

Even if Ofcom is willing to break British citizens' human rights, there are a litany of practical concerns with the application of Technology Notices.

(1) Service Providers will cease operations in the UK, leaving only unencrypted messaging platforms or North Korean-style government-backed communications app

WhatsApp and Signal have said they will leave the country rather than implement the accredited technology described under the Online Safety Act.[4] The UK provides WhatsApp with less than 2% of their three billion global customer base,[5] and both have supported Apple in their legal battle with the Home Office in 2025, with WhatsApp even acting as Intervenor:

> *"WhatsApp would challenge any law or government request that seeks to weaken the encryption of our services and will continue to stand up for people's right to a private conversation online"*

Meanwhile, the Trump administration has threatened to increase tariffs on countries that "discriminate" against US tech.[6] So immediately the UK would be left without the messaging apps that its own government uses, and may even face economic hardship as a result of the decision. Leaving only non-encrypted and unsafe communications apps, or a government-backed North Korean-style app like *Kangsong* or *Koryolink* which are developed and controlled by the state.[7]

(2) Let's say Service Providers didn't leave the UK, enforcing the new regime will create technological issues for users that require consensual or covert installations

The options available under the new regime for UK users of private communications with accredited technology are to (a) get users to consent to installing such accredited technology on their devices which scans all of their messages, or (b) install the technology covertly or deceitfully.

Given that the vast majority of UK citizens use E2EE, they will have to confirm that they are happy to have CSS installed on their private communications channels - i.e. their phones and

[4] *www.theguardian.com/media/2023/sep/06/whatsapp-signal-online-safety-bill-uk-encryption-privacy*
[5] *techcrunch.com/2025/05/01/whatsapp-now-has-more-than-3-billion-users/?utm_source=chatgpt.com*
[6] *www.theguardian.com/us-news/2025/aug/26/donald-trump-tariffs-us-tech-uk-digital-services-tax-eu*
[7] *www.dailynk.com/english/exclusive-rare-look-north-korea-official-smartphone-apps/?utm*

laptops - which will have to be confirmed via the Service Provider and/or by government notice. Given that two of the UK's leading parliamentary permissions at the time of writing concerns (a) repealing the Online Safety Act[8] and (b) not introducing digital ID cards[9], it is impossible to see how this is implemented without a huge battle and headache for the government.

Alternatively, the technology could be installed without the consent of users - exposing those adding the technology to ethical and legal disputes on behalf of citizens and human rights campaigners.

(3) We'd need to successfully filter over 1.3 trillion messages each year in the UK. Who is in charge of this? US tech companies? The police? The UK government? Global contractors?

The Online Safety Act does not grant any new resources to the police. There is no guarantee that people assessing false positives would be UK citizens, and many content moderators demonstrate a range of psychological harms from the job including symptoms consistent with experiencing repeated trauma.[10]

If just 0.001% of 1.3 trillion messages are flagged each year, that's 13 million messages to sift through in total - or 35,616 a day. Once flagged, these require human assessment, which would necessitate the invasion of privacy of false positives (so-called "bycatch"), before being sent on to law enforcement. Notably, only CSEA content needs to be reported to law enforcement - meaning the impact on Article 8 and Article 10 rights conducted while scanning for terrorism content would not even lead to convictions with respect to terrorism content.

Further, S. 121 OSA places the burden of determining whether content should be removed in the hands of private technology companies. It has already been shown that instead of risking huge potential fines for non-compliance, technology companies are over-censoring content to comply with other duties under the OSA.[11] As highlighted by Gavin Millar KC in his legal opinion, determining whether the terrorism and CSEA offences included in the OSA have been committed would be difficult even for law enforcement or judges - the prospect of tech company employees accurately doing so are incredibly remote. Overcensoring would further aggravate the impact that Technology Notices would have on user's freedom of expression.

---

[8] *'Repeal the Online Safety Act', UK Government and Parliament, accessed October 7, 2025. Available at: https://petition.parliament.uk/petitions/722903.*
[9] *'Do not introduce Digital ID cards', UK Government and Parliament, accessed October 7, 2025. Available at: https://petition.parliament.uk/petitions/730194.*
[10] *https://cyberpsychology.eu/article/view/33166*
[11] *guardian.com/commentisfree/2025/aug/09/uk-online-safety-act*

There is no guarantee that the evidence collected would lead to a criminal conviction. In fact, the collection of messages which contain personal data may put Service Providers in breach of their GDPR obligations themselves, increasing crime rather than stopping it.

(4) Technology Notices would introduce weaknesses to the security of E2EE systems, meaning bad faith actors could access the private communications of citizens, journalists, dissidents, vulnerable groups, security personnel, and parliamentarians.

Chinese state actors exploited similar vulnerabilities used by US forces to wiretap suspects. Salt Typhoon, as the hack was called, "compromised the private portals, or backdoors, that telephone companies provide to law enforcement to request court-ordered monitoring of phone numbers."[12]

The Cybersecurity and Infrastructure Security Agency (CISA) has urged highly targeted individuals - senior officials, journalists, political leaders - to use end-to-end encrypted tools like Signal to protect themselves.[13]

In the last Parliament, over two-thirds of parliamentary offices had their personal information exposed on the dark web: 117 LinkedIn profiles, 2,110 email accounts, 216 passwords, 21 Facebook accounts, 21 Twitter handles, and 16 Instagram profiles were all stolen.

Element.io is a British, encrypted communications platform used by HM Government, NATO, and the United States Marine Corps. They explicitly provide end-to-end encryption by default. They said in a post about the OSA-

> *"By forcing this 'backdoor' into E2EE, the resulting surveillance mechanisms would be able to access anyone's messages, at any time, forwarding them to the authorities if suspected as illegal. This weakens security for everyone; from the 99 percent of normal law-abiding people through to businesses and governments."*[14]

(5) This opens the door to abuse by future UK governments who can use these powers in tandem with the IPA to target journalists, minority groups, and dissidents.

Once 'Accredited Technology' is used to break encryption, the Home Office has the power to use "bulk surveillance warrants" under the IPA, providing them with access to encrypted private messages en masse for the first time.[15]

---

[12] *University of Maryland*
[13] *Reuters*
[14] *https://element.io/blog/the-online-safety-bill-an-attack-on-encryption/*
[15] *indexoncensorship.org/2023/09/online-safety-bill-loophole-opens-door*

If you would like more information and to discuss encryption with the experts, please contact indexencryption@89up.org

Before the implementation of the Online Safety Act, we had both technological (via encryption) and legal protections against abuse of powers akin to mass surveillance. By removing the technological barriers with use of technological notices, this leaves us only with legal defences and therefore a vulnerability to future political and governmental exploitation.

These unprecedented powers leave the door open to abuse by future governments who can potentially utilise IPA powers to target political dissidents, members of the LGTBQA+ community, or immigrant populations, for example.

(6) Ofcom and the UK government would face litigation from across the globe

Ofcom's powers extend to all private communications made in the UK, including those made with people overseas and using platforms provided by overseas companies. This means service providers will have a choice of leaving the UK market, complying with UK law, or challenging Ofcom's jurisdiction within international jurisdictions.

Ofcom has already been summoned to a US court to answer questions over enforcement of the Online Safety Act against American companies.[16] Given the effect of Technology Notices will span all jurisdictions globally, there is nothing to stop companies or governments from launching legal proceedings against Ofcom to protect its citizens and/or financial interests. This will have severe consequences for the UK's diplomacy, trade, and international standing, as we have already seen with senior members of the US administration - Tulsi Gabbard, Director of National Intelligence, and JD Vance, Vice President - using "back doors" to encryption as a wedge issue with the UK government.[17]

(7) Introduction of Technology Notices are likely to disproportionately impact vulnerable and minority groups, in contravention with the Rule of Law

CSS treats all users as potential perpetrators rather than focusing on suspicion-based monitoring, it cannot reliably determine the context in which material appears and whether it is abusive, consensual, or part of a report by a victim - leading to the overflagging of vulnerable groups (e.g. victims of domestic abuse, LGBT+ users, children, and activists):

> "CSS would need to operate in such a way that errors in the decision-making process do not disproportionately affect minorities. This includes, among others, errors due to algorithmic bias, which are known to increase racial inequality, and errors due to a lack

[16] *https://www.bbc.co.uk/news/articles/clyjq40vjl7o*
[17] *https://www.bbc.co.uk/news/articles/cdj2m3rrk74o*

of context when making decisions that can create major disadvantages, e.g. for queer kids."[18]

This means Article 8 and 10 rights would be disproportionately affected by the exercise of Ofcom's powers under s.121 OSA. It would also take away the possibility to communicate securely for groups who depend on the privacy of their communications for their safety, increasing the risk of them being targeted by authoritarian regimes, far right extremists, or others who wish them harm.

This fundamentally undermines the Rule of Law because it shifts power away from transparent, legally constrained systems toward opaque, pre-emptive surveillance controlled by private companies or other citizens.

The Rule of Law depends on clear, predictable rules so citizens can understand what conduct is lawful. CSS introduces technological uncertainty.

It allows for pre-emptive enforcement of norms or laws without prior legal scrutiny - secretive criteria, incompatible with principles like due process, transparency, and access to justice.

If people believe their private communications are being scanned, they are more likely to self-censor, particularly those in vulnerable or minority groups. This results in a curtailment of legitimate political speech, journalism, advocacy, and has a chilling effect on expression across the board.

Recommendations

Simple fixes Ofcom can implement today

- **Remove 'Technology Notices' from the Online Safety Act in their entirety.**
- **Prevent technology notices from applying to private messaging services.**
- **Amend Section 121 of the Online Safety Act to require judicial oversight for the issuance of any technology notices (as opposed to a 'skilled persons report').**
- **Remove encryption from Ofcom's risk register under the Online Safety Act.**

[18] *academic.oup.com/cybersecurity/article/10/1/tyad020/7590463?utm*

If you would like more information and to discuss encryption with the experts, please contact indexencryption@89up.org