INDEX ON CENSORSHIP

A VOICE FOR THE PERSECUTED

ONLINE SAFETY, OR SURVEILLANCE

HOW A LOOPHOLE IN THE ONLINE SAFETY BILL OPENS THE DOOR TO UNPRECEDENTED INVESTIGATORY POWERS

SEPTEMBER 2023

This report raises the alarm over a loophole in the Online Safety Bill that will open the door to the unprecedented and chilling surveillance of British citizens under the Investigatory Powers Act.

Clause 122 of the Online Safety Bill provides Ofcom the means to break encrypted messaging services through 'technology notices' served without legal oversight. Once 'Accredited Technology' is used to break encryption, the Home Office has the power to use "bulk surveillance warrants" under the Investigatory Powers Act: providing access to encrypted private messages **en masse** for the first time.

Without urgent clarification in Parliament, there is a risk that security services such as MI5 can compel technology companies who operate encrypted messaging services to interfere with user communications or acquire masses of data in secret. There is no clarity to date on whether Ofcom would be notified under such circumstances nor whether Ofcom themselves could be subjected to a bulk surveillance warrant as a result of the data insights they gain in their role as an independent regulator.

The long-standing campaign against the use of encryption technology has now seemingly culminated in a two-pronged legislative attack against British rights to privacy and freedom of expression. This report outlines the (1) meaning of new enforcement powers under the Online Safety Bill, (2) the Surveillance Gateway that is being opened, (3) proposed reforms to the Investigatory Powers Act and (4) the key questions that Parliament urgently needs answers on.

On **Monday, 11 September 2023**, the House of Commons will review the Online Safety Bill for the first time in nine months in which they will decide whether they accept the Government's amendments to introduce mass surveillance on British people and to sign off on a massive curtailment of journalistic freedoms.[1]

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

This is Members' **final chance** to:

	Action	Issue
a)	Amend Clause 122 of the Online Safety Bill	To require judicial oversight for the issuance of any technology notices (as opposed to a 'skilled persons report')
b)	Ask for Government clarification at the despatch box	For assurances that the Government will not allow for the use of technology notices under powers of the Investigatory Powers Act

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

Online Safety Bill
Section 122 Notices

The Online Safety Bill, as currently drafted, gives Ofcom the powers to impose Section 122 notices on the operators of private messaging apps and other online services. These controversial notices can impose algorithmic content detection tools that include the surveillance of the private correspondence of UK citizens.[2] The proposed powers mandate unproven technologies such as **'Client Side Scanning'** to be implemented with limited legal safeguards. It means the UK would be one of the first democracies to place a de facto ban on end-to-end encryption for private messaging apps.[2] The move has been met with derision from technology platforms, many of whom have said they will remove services from the UK rather than impugn their security infrastructure as a result of the new enforcement powers.[3]

No communications in the UK - whether between MPs, between whistleblowers and journalists, or between a victim and a victims support charity - would be secure or private if end-to-end encryption is unavailable. In an era where Russia and China continue to work to undermine UK cybersecurity, Index on Censorship believes this could pose a critical threat to UK national security.

A legal opinion we commissioned in November 2022 by **Matthew Ryder KC** found that:

- *Section 122 notices install the right to impose technologies that would intercept and scan private communications on a mass scale. The principle that the state can mandate the surveillance of millions of lawful users of private messaging apps should require a higher threshold of justification which has not been established to date.*
- *Ofcom could impose surveillance on all private messaging users with a notice, underpinned by significant financial penalties, with less legal protections than equivalent powers under the IPA.*
- *The proposed interferences with the rights of UK citizens arising from surveillance under the Bill are unlikely to be in accordance with the law and are open to legal challenge.*
- *Journalists will not be properly protected from state surveillance risking source confidentiality and endangering human rights defenders and vulnerable communities.*

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

In response to these concerns, at Report Stage in the House of Lords, the government introduced the requirement for a **'Skilled Persons Report**' under Section 122 of the Bill.[4] In our view, this level of oversight is insufficient for the proposed bulk surveillance regime given the depth, sensitivity and complexity of the legal and technology issues concerned, including fundamental rights under common law and the European Convention on Human Rights.

We do not view the 'Skilled Person' safeguard as sufficient or satisfactory especially given some of the recent developments (highlighted below) in the law of surveillance which raise further questions about the intersections of proposed new legal frameworks.

Surveillance Gateway
Ofcom and Accredited Technology

If **Client Side Scanning** is mandated under Ofcom's new enforcement powers in the Online Safety Bill it will open the technological gateway for UK security services to use 'bulk surveillance warrants' under the **Investigatory Powers Act 2016** to surveil encrypted private messaging for the first time.

This is because, at present, security services are unable to access end-to-end encrypted messaging on a mass (as opposed to targeted) scale given that individual messages are encrypted and the content of the messaging is unavailable to the platforms themselves. If Parliament now legislates that Ofcom can force technology companies to scan all users' devices, it will open up the technical capability for a bulk surveillance warrant to be implementable.

This development comes at a time when the conduct of security services and the **Home Office** in relation to bulk surveillance powers have been found to be unlawful. The Investigatory Powers Tribunal ruled in January 2023 that from late 2014 until 2019, MI5 held large amounts of data unlawfully because, contrary to law, at least one of the agency's technology systems lacked proper retention, review and deletion ('RRD') safeguards.[5] The three-judge body also found "serious failings in compliance with the statutory obligations of MI5 from late 2014 onwards", adding that "those failings ought to have been addressed urgently by the management board [of MI5]".

The IPT also concluded that the Home Office had overlooked the agency's failings, neglecting to make "adequate enquiries" or investigate long standing compliance risks, despite red flags being reported several times since December 2016. The judges said the Whitehall department:

> ***"did not have grounds to be satisfied that effective safeguards applied to warrants where there had been no assessment or effective investigation into compliance with RRD". "We have made findings of serious failures by MI5 and the secretary of state," the IPT said, adding that there had been a "widespread corporate failure".***[6]

The government insists that the two legislative regimes of the Online Safety Bill and the IPA exist in completely separate worlds with the former concerned only with CSEA content in private messaging and the latter with national security and bulk personal datasets. We consider looking across the legislative framework they are creating, they are painting a picture of a very different world of surveillance for UK citizens.

Law Reform

The Investigatory Powers Act

It seems that the government's solution to hitherto failures in safeguarding will be addressed by in effect loosening them in statute. Reform of the IPA now sits with the Home Secretary following an independent review completed by **Lord Anderson KC** and the Home Office consulting on a raft of changes.[7] A precis of recommendations for IPA law reform include that:

- *non-UK-based companies comply with changes that would affect their product globally - such as providing a backdoor to end-to-end encryption*
- *action to be taken immediately if a notice to disable or block a feature is received from the Home Office, rather than waiting until after the demand has been reviewed or appealed against*
- *where necessary, relevant operators to inform the Secretary of State of relevant changes, including technical changes (notification to be made a reasonable time before relevant changes are implemented which was highly criticised by Apple)*
- *a new, light touch regulatory regime is created for the retention and examination by the UK Intelligence Community (UKIC) of bulk personal datasets in respect of which individuals have a low or no expectation of privacy (Lord Anderson)*

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

- *the law on investigatory powers be updated to find a new legal framework which is appropriate to developments in technology such as AI and which address the two main challenges the Home Office has identified (i) the bar on using intercept material as evidence in legal proceedings; and (ii) the challenge posed by the move to end-to-end encryption (Lord Anderson)*

Lord Anderson (who has proposed the introduction of a low/no privacy datasets based on the four principles suggested by UKIC)[8] has also recognised that there needs to be an evolution of the right to privacy when the IPA is amended and as technology evolves:

- *The IPA's focus on how bulk data may be acquired or retained may need to evolve towards a focus on how bulk data is used – not simply by improved oversight of selectors but by increasingly sophisticated bulk analytics and AI techniques that are applied to personal data.*
- *In the context of ML models in particular, the IPA's focus on the right to privacy may need to be broadened to reflect more fully the other data rights that can be impacted by biassed or poorly-trained models, including transparency, algorithmic fairness and non-discrimination.*
- *This in turn has implications for oversight: it is for consideration whether the Information Commissioner's Office (ICO) with its special expertise in data processing and AI should have an enhanced role in intelligence oversight, alongside IPCO.*

Key Questions
For the House of Commons

With **Third Reading** of the Online Safety Bill in the Lords, on 6th September 2023 and the Commons' consideration of Lords amendments shortly thereafter, there are two key opportunities for (a) Peers to once again put questions to the Minister - seeking clarifications and statements on legislative intent / unintended consequences and (b) for government to rectify their proposed amendments by engaging in a constructive dialogue and taking action to clarify ambiguities.

In particular, the Minister(s) should clarify:

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

1. *Could technology companies subject to a section 122 notice, and a requirement to use 'accredited technology' be then subject to a bulk interception or acquisition warrant under the IPA in relation to private messaging?*
2. *Could datasets obtained from an accredited technology such as client side scanning of devices be capable of constituting the proposed low/no dataset and therefore be subject to minimal scrutiny in order to be obtained by security services?*
3. *If technology platforms declare to users that they 'co-operate with lawful requests to access user data including private messaging' under their new obligations under the Online Safety Bill are they therefore implying low/no expectation on privacy?*
4. *Is there any other jurisdiction that has a defined category of low/no datasets as opposed to 'publicly available' datasets? Is this approach compliant with EU law / the EU-UK Data Adequacy Agreement?* [9]

Conclusion
Online Safety or Surveillance?

Index on Censorship is concerned that the era of binary privacy i.e. that something is either communicated privately or it is not, exemplified through the proliferation of the use of end-to-end encryption, is being forced into a non-binary political debate.

Privacy is becoming a 'spectrum' in which the government can potentially infer user expectation on privacy through the guise of tackling societal harms such as CSEA content / national security and with scant regard to existing international human rights law.

This has concerning implications given the data processing powers of developing AI technology and the hitherto failures of the Home Office and security services under the limited oversight of surveillance under the IPA.

Parliament needs to urgently guard against passing new legal frameworks that deny UK citizens the privacy protections that US and EU citizens are afforded by their respective constitutional courts.

If you would like more information or to discuss the arguments around these clause further, please contact hello@legaltosaylegaltotype.uk

Endnotes

1. https://shorturl.at/sHKN2

2. https://techcrunch.com/2023/07/05/uk-online-safety-bill-risks-e2ee/

3. https://shorturl.at/wyILU

4. The idea of a 'skilled person' is borrowed from the Financial Conduct Authority under the Financial Services and Markets Act (FSMA) (as amended by the 2012 Act). Under section 166 FSMA, the regulator has the power to require a firm to appoint a 'Skilled Person' to produce a report on specified matters or to appoint a skilled person directly. This could be, for example, a review of past business in a particular area or sales of a particular product; a review of a firm's compliance with the client money and asset rules; or a review of a firm's systems and controls.

5. https://shorturl.at/dikES

6. https://www.ft.com/content/e3533128-90f4-4746-a419-a025ee2728be

7. https://shorturl.at/qAKWX *"The intelligence agencies are arguing for a reduction in the safeguards regulating their use of large volumes of information, known as bulk personal datasets (BPDs). These datasets often contain information, some of which may be sensitive, about extremely large groups of people, most of whom are unlikely to be of intelligence and security interest. MI5, MI6 and GCHQ frequently use BPDs that are drawn from a wide range of closed and open sources and can also be acquired through covert means.The agencies, who argue these datasets help them identify potential terrorists and future informants, want to relax rules about how they use BPDs in which they believe people have a "low or no expectation of privacy".*

8. A. nature of the data: the extent to which the nature of the data is such that an individual to whom the data relates would be considered to have a reasonable expectation of privacy;
B. data subject: the extent to which there is evidence (i) that the data has been manifestly made public by the data subjects, or (ii) that the data subjects have consented for the data to be made public; C. publication: the extent to which the data has been published subject to editorial control and/or the application of professional standards, and how widely known the dataset is; and D. use (or further use): the extent to which data has been used already in the public domain such that further use by UKIC for the purpose of its functions is unlikely to lead to further intrusion.

9. https://techcrunch.com/2023/05/09/eu-scam-scanning-unlawful-advice/