# Investigatory Powers (Amendment) Bill: Written Evidence

Internet Society, Internet Society UK England Chapter, Access Now

7 March 2024

The Internet Society and its UK Chapter submitted a response to the initial consultation on the Investigatory Powers (Amendment) Bill, in June 2023, setting out a broad range of concerns about potentially harmful effects of the proposals.[1] The concerns we outlined persist: they include harmful impact on the security of the Internet, which, in turn, compromises the security of citizens, the trustworthiness of UK online services, and the digital economy.

**In this briefing document, the Internet Society, its UK Chapter, and Access Now limit our input to the proposed change to the notices regime as set out in S21 inserting S.258A, and its implications for end-to-end encrypted services. We believe that, despite the then Home Secretary's claims to the contrary, this Bill does indeed give the Secretary of State new powers to prevent technology companies from deploying end-to-end encryption, or require them to introduce systemic vulnerabilities in order to decrypt or compromise messages, and this would in turn create new security risks. We would like to make Members of Parliament aware of these risks before they pass this legislation, and we voice concerns about the legislative process for this Bill, which has severely limited the submission of evidence, and prevented that evidence from being properly considered by both Houses.[2]**

## Summary

'Telecommunications operators' based abroad will have to comply with law enforcement access requests from UK authorities; the Bill's definition of 'operators' is so broad as to include Internet-based services. They will be required to notify the government when they make changes to their systems, including security patches and improvements, if those changes close a loophole which is currently being exploited for law enforcement access. Preventing or delaying patches to security flaws runs

[1] Written Evidence from Internet Society, Internet Society UK England Chapter: https://isoc-e.org/the-revised-ipa-2016-consultation-response/

[2] For example, Bill went through its Report state in the Lords before the Joint Committee on Human Rights had even been able to submit its report on the Bill; the Equalities and Human Rights Commission was unable to fulfil its statutory duty to report on the Bill; and civil society organisations have struggled to respond to calls for evidence, given the unseemly haste with which the Bill has been pushed through Parliament so far.

against every principle of good practice, including the advice of the UK's National Cyber Security Centre.[3]

It is technically not feasible for end-to-end encrypted services to comply with law enforcement access requests without causing collateral damage to other users who are not themselves subjects of an investigation. Law enforcement access on demand requires either the ability to inspect the contents of an individual's device before they are encrypted, or the ability to neutralise the encryption once it has been applied. Both these approaches introduce systemic flaws, creating a surveillance capability which, by definition, fails the proportionality test.

## Notification of changes to telecommunications services

We are providing evidence in respect of S. 21 of the IPAA[4] inserting a new section 258A [*Notification of proposed changes to telecommunications services etc.*]. This amendment to the Notices regime seeks to protect 'lawful access' to the networks and systems run by telecommunications operators. The term 'lawful access' generally refers to a mandate for law enforcement and the intelligence services to access encrypted content transmitted over networks or to ask service providers to do it for them.[5] The Secretary of State referred to 'lawful access' several times at the Second Reading, for example *"rolling out technology that precludes lawful access,"*[6] and we infer that it has this meaning. The use of the term 'lawful access' in this context is dangerous, as the term sounds reasonable but in fact disguises the actual complexity of the issue, including the potential harm to wide sections of the public when encryption is compromised.

New section 258A creates new powers for the Secretary of State to require that operators give advance notice of changes to their systems, if those changes affect the operator's ability to satisfy a law enforcement access request. Such changes could be to encrypt a service that is currently not encrypted, to improve other aspects of product security, or to patch newly-discovered security flaws. It is supplemented by S.18, which would require operators to delay making changes (and, by implication, security improvements) to their system while an objection lodged by the operator is being reviewed.

Software updates, also called patches, are a primary means of addressing vulnerabilities in operating systems, applications, and devices. These updates are regularly released by software developers to fix bugs, and, most importantly, patch security holes. It is critical that security vulnerability updates get implemented before bad actors including hackers and terrorists exploit them and the requirement for advance notices is incompatible with these time critical processes, thus creating a major security risk.

---

[3] https://www.ncsc.gov.uk/blog-post/the-problems-with-patching

[4] Bill as brought from the House of Lords https://publications.parliament.uk/pa/bills/cbill/58-04/0157/230157.pdf.

[5] Internet Society, Info Guide: 6 Ways "Lawful Access" Puts Everyone's Security at Risk https://www.internetsociety.org/resources/doc/2019/factsheet-for-policymakers-6-ways-lawful-access-puts-everyones-security-at-risk/

[6] House of Commons Hansard, 19 February 2024, column 522, 523, 524, James Cleverly

Crucially, the Government refused, during the Lords' debate, to set a time limit for an operator's appeal against a notice to be resolved by the Secretary of State. This means the Secretary of State can force an operator to leave an insecure system in place indefinitely, simply by doing nothing.

The new section 258A would apply not only to telecoms operators based in the UK, but also those based abroad and who provide telecoms services in the UK.[7] This is achieved via S.19 (2)(b) which amends the definition of a 'telecoms operator'. These overseas telecommunications operators are understood to refer to a range of platforms like Meta, WhatsApp, Apple, Signal, and Telegram, and the services offered could include encrypted services.

This raises serious concerns. If the government were to press ahead with notifications to encrypted services, it risks doing damage to the global infrastructure that is designed precisely with the intention of keeping people safe. To comply with a lawful access requirement, these companies would have to introduce systemic weaknesses and vulnerabilities in their services, such as security 'backdoors', exposing users to the risk of their phones being compromised. Further, it will stifle innovation in the burgeoning online privacy and security landscape, undermine the resilience of the cybersecurity infrastructure that people and institutions in the UK rely on, and ultimately cause harm to people's rights, national security, and the economy.

It is not possible to monitor specific content on an end-to-end encrypted service without creating indiscriminate interference with the privacy of other users who are not the target of the measures. This raises the issue of proportionality. Around 65 per cent of adults in the UK use WhatsApp as their main communications service, according to research published by Ofcom in 2023.[8] Building a surveillance capability into WhatsApp, capable of satisfying any access request from UK law enforcement, would introduce a systemic security vulnerability with disproportionate impact on law-abiding users. The UK risks making itself the weak link in the chain of secure communication, endangering law-abiding users outside the UK communicating with those inside the UK. The proposed amendments simply do not take into account the reality of a global Internet, let alone the safety, security and rights of non-UK users at risk from authoritarian or oppressive regimes in their own countries.

## Legislative process

As in our evidence submitted to the Joint Committee on Human Rights,[9] we voice concerns over the procedure followed, as the deadline for written evidence is the same day as the Committee scrutiny of the Bill, and a little over a week from the publication of the call for evidence. The deadline for amendments was apparently midday on 4 March. We question the Joint Committee's ability to process

[7] IPAA, S.19 (2) (b) controls or provides a telecommunication system which— (i)is not (wholly or partly) in, or controlled from, the United Kingdom, and (ii) is used by another person to offer or provide a telecommunications service to persons in the United Kingdom." ]

[8] Ofcom Communications Market Report 2023 https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/2023/interactive

[9] Written Evidence From Freedom From Internet Society, Internet Society UK England Chapter (Ipa0005) https://committees.parliament.uk/writtenevidence/127896/html/

submissions and provide informed input to the policymaking process with such tight deadlines, risking insufficient diligence, especially when it comes to human rights implications.

## Recommendations

In response to our concerns about S.21 of this Bill, we recommend:

1. To include explicit safeguards (such as a prohibition on introducing systemic vulnerabilities) to prevent unsafe use of the resulting powers and risk compromising the security of end-to-end encrypted services.
2. To ensure that any revision of the IPA demonstrates how its operation and enforcement will comply with the necessity and proportionality principles.
3. To require that impact assessments on fundamental rights and privacy are conducted, and properly reflect the legitimate interests of all stakeholders, before telecoms operators can be required to make any adjustments to their systems or alter their plans for deployment of security-related functions.
4. To perform an economic impact assessment in relation to UK online business and innovation, especially the effect of laws that will undermine overseas trust in UK online services and UK-developed products, at a time when the UK can ill afford further blows to the economy.

## Law enforcement access and systemic risk

Law enforcement access would require providers to seek out, identify, and forward or remove content at the request of law enforcement agencies. This is technically not feasible on encrypted platforms without simultaneously inserting systemic vulnerabilities into the system that risk collateral damage to users who are not the target of law enforcement investigations.

A systemic vulnerability is one that extends beyond the targeted device or service that an individual user is using and is implemented such that any other user could be affected. These vulnerabilities would create systemic effects across the global Internet ecosystem, resulting in the compromise of devices and systems, and unauthorised access to data. The outcome would be an unsafe and chaotic online environment and a new canvas for criminals to exploit. In the new AI environment, full of as-yet poorly understood opportunities and risks, this reads as a recipe for failure.

Even if access is provided under a warrant, the effect is the same. Providers of encrypted communications services cannot read, see, or hear the content of the messages they transmit. For encrypted platforms to be able to comply with demands for access to data, they would need to introduce measures to obtain data that they currently have no access to. The introduction of any such measure—whether it is called a backdoor, or an exceptional access mechanism for decryption or

interception, or client-side scanning—would mean that the platform, in its entirety and for all its users, ceases to be encrypted. It means an end to the citizen's ability to hold a confidential conversation at a distance, or to transact securely online. In an information society, with a data-driven economy, and global commerce, this should be unthinkable.

Client-side scanning multiplies the systemic risks. It is fundamentally at odds with privacy and security, reaching pre-emptively into the phones and computers that are essential to citizens' everyday lives. It is also vulnerable to reverse engineering and evasion, rendering it ineffective. Ineffective law enforcement mechanisms fail the "necessity" test, since a mechanism that doesn't work is by definition unnecessary.

Client-side scanning introduces inefficiency, increasing network traffic and requiring extra processing which, on the devices of a law-abiding user, is in any case pointless. It increases the 'attack surface' that bad actors can exploit and exposes millions of people's phones to intrusion by unauthorised entities, such as hostile foreign states. A content-scanning mechanism, once in place, can be subverted for purposes that go far beyond any democratically acceptable law enforcement remit, such as censorship, tracking, and consent-less facial recognition.[10]

In the case of Australia, draft industry standards framed by the eSafety Commissioner, have been criticised on the basis that they threaten encryption; in response, the Commissioner has provided a categorical reassurance that the standards "will not require industry to break or weaken end-to-end encryption, monitor the text of private communication or indiscriminately scan large amounts of personal data."[11]

It must be noted that the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018[12] (TOLA) is subject to ongoing review by Australia's Parliamentary Joint Committee on Intelligence and Security and by the Independent National Security Legislation Monitor. The UK should not make itself an outlier by ignoring the rights-respecting recommendations stemming from these reviews and other stakeholders.

## Lawful access and proportionality

The clearest signal yet, that lawful access could be unlawful on an end-to-end encrypted service has come from the European Court of Human Rights. In a recent judgement,[13] the Court confirmed that an

[10] Volume 4, footnote 197 *Jain, S., Cretu, A., Cully, A., and de Montjoye, Y., 2023. Deep perceptual hashing algorithms with hidden dual purpose: when client-side scanning does facial recognition.*

[11] https://www.esafety.gov.au/industry/codes/standards-consultation

[12] Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 https://www.legislation.gov.au/C2018A00148/latest/text 317ZG

[13] European Court of Human Rights, Podchasov v. Russia. (Application no. 33696/19) Judgement 13 February 2024 https://hudoc.echr.coe.int/eng/#{%22itemid%22:[%22001-230854%22]}

order requiring data from users to be detected and identified for law enforcement purposes, would not meet the proportionality test. This is because it is not possible to monitor specific users' content, without affecting the rights of others on the network. Interference with privacy would be collateral damage.

The rights at stake are the right to freedom of expression and privacy. The lawfulness of the interference must be balanced against arbitrary interference with the fundamental human rights of other users. The Court noted that, on an encrypted service, in order to read the content of one user, providers have to install software—either through a backdoor on the server or on the end-user devices—that will indiscriminately impact all users. The Court ruled that such a requirement would be disproportionate. The principles set out in the judgement would apply to any instance where a service was asked to break, weaken, or compromise end-to-end encryption.

In the absence of full and timely input from the JCHR (because of the bill's rushed progress), and of *any* evidence from the EHRC (apparently due to budgetary constraints), we believe it is unsafe to assert that the Bill complies with the UK's obligations regarding human rights compliance.

Anyone tempted to take that assertion at face value should bear in mind that, for years, the UK maintained that its surveillance regime satisfied the necessity and proportionality requirements of laws to which it remains a signatory—and that Snowden's disclosures demonstrated, to the satisfaction of the courts, that this was not the case.

## About Us

The **Internet Society** is a global charitable organization that advocates for an open, globally connected, secure, and trustworthy Internet. We work with our community of over 115,000 individual members as well as 129 Chapters and Special Interest Groups in pursuit of an Internet that works for everyone.

The **Internet Society UK England Chapter**[14] is a local chapter of the global Internet Society, a non-profit organization that works to build, promote, and defend the Internet. The chapter was founded in 1999, incorporated in England and Wales (Company number 10644428) and has thousands of supporters who share an interest and a vision of an open and user-centric Internet for everyone. The chapter organizes and participates in various activities and events, such as educational workshops, community programs, public policy initiatives, and networking opportunities. The chapter also collaborates with other chapters, special interest groups, and stakeholders to address the challenges and opportunities of the Internet in the UK and beyond.

**Access Now** is an international non-profit organization which works to defend and extend the digital rights of users at risk globally. Through presence in more than 13 countries around the world, Access

[14] https://isoc-e.org/

Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Access Now also operates a 24/7 digital security helpline that provides real-time, direct technical assistance to users around the world.