BIG BROTHER WATCH

Big Brother Watch response to Home Office consultation on revised notices regimes in the Investigatory Powers Act 2016

July 2023

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Mark Johnson

Advocacy Manager

Email: mark.johnson@bigbrotherwatch.org.uk

INTRODUCTION

1. Big Brother Watch welcomes the opportunity to respond to the Home Office's consultation on revised notices regimes in the Investigatory Powers Act 2016.

2. Since the Investigatory Powers Act (IPA) was first introduced to Parliament as a Bill, Big Brother Watch has opposed the bulk surveillance powers set out in the legislation as failing to meet the crucial human rights tests of necessity and proportionality.

3. The changes to notice regimes under the IPA, proposed by the Home Office, appear to be set out in a way which could be used to prevent communications platforms from adopting or rolling out end-to-end encryption, or other privacy-preserving technologies, across their services.

4. These proposals engage the fundamental rights to privacy and freedom of expression, protected by Articles 8 and 10 of the European Convention on Human Rights (ECHR) respectively. The ECHR is clear that interference with these rights will only be lawful where they are provided by law, necessary and proportionate.[1][2] The presumption must rest in favour of protecting these rights and interference with them should come as a last resort.

5. It is well documented that the Home Office sees end-to-end encryption, the technology that keeps our messages private and secure, as an inherent threat to national security. This has been demonstrated by the Home Office's condemnation of Meta's decision to encrypt its messaging service[3], important context to the proposals discussed here, as well as the Department's influence over the Online Safety Bill to include provisions which engage private messaging services[4].

6. This framing fails to recognise privacy and security as mutually reinforcing concepts or take into account the benefits end-to-end encryption can provide in keeping people's communications safe from hackers and criminals. Private communications are fundamental for our safety and privacy – and are also critical for protecting journalists, human rights activists and whistleblowers in the UK and all around the world.

7. It is important to note that those using end-to-end encrypted messaging services are not above the law. Law enforcement agencies in the UK possess

1 Article 8: Respect for your private and family life, Human Rights Act 1998, EHRC, https://www.equalityhumanrights.com/en/human-rights-act/article-8-respect-your-private-and-family-life

2 Article 10: Freedom of expression, Human Rights Act 1998, EHRC, https://www.equalityhumanrights.com/en/human-rights-act/article-10-freedom-expression

3 Braverman writes to Zuckerberg expressing concerns over Meta's encryption plans, Independent Online, 3 July 2023, https://www.independent.co.uk/news/uk/politics/mark-zuckerberg-meta-home-secretary-suella-braverman-commons-b2368632.html

4 Online Safety Bill: Home Secretary's op-ed for The Telegraph, Home Office, 6 July 2022, https://www.gov.uk/government/news/online-safety-bill-home-secretarys-op-ed-for-the-telegraph

a wide range of powers to obtain information at device level including by seizing devices, compelling passwords, and even covertly monitoring and hacking accounts to overcome security measures and identify criminals.

8. This response concerns where these proposals pose threats to the fundamental rights to privacy and freedom of expression. We are concerned that the consultation's proposals lack detail and do not outline the specific legislative mechanisms by which the changes will be made. The proposed changes would grant the Secretary of State significant new powers and could have a serious detrimental impact on the privacy and security of private communications. No legislative proposals should be brought forward without a detailed, thorough public consultation.

OBJECTIVES 1 AND 4 – STRENGTHENING THE NOTICE REVIEW PROCESS AND NOTIFICATION REQUIREMENTS

9. Objective 1 refers to the process surrounding the issuing of a Technical Capability Notice under the IPA framework. It states:

> *"If at this point the operator is dissatisfied with the terms of the notice they have a statutory right to refer the notice (or part of it) to the Secretary of State for review.*
>
> *As it stands, during a review period the operator is not required to comply with the notice, so far as referred, until the Secretary of State has concluded the review. Where an operator is seeking to make changes to their system that would have a detrimental effect on a current lawful access capability, this could create a capability gap during the review period, which is an issue we believe should be addressed.*
>
> *This could be done through a general requirement to maintain the status quo through this period, ensuring that our lawful access to data is maintained.*
>
> *This would be without prejudice to the outcome of the review process."*

10. This appears to infer the creation of powers to halt a service updating its security by using tools such as end-to-end encryption while a review is taking place.

11. Objective 4 creates new obligations on service providers, compelling them to notify the Secretary of State of any technical changes they intend to make to

the digital infrastructure of their services. The third paragraph of this section reads:

> *"We therefore propose that a provision should be introduced to require, where necessary, relevant operators to inform the Secretary of State of relevant changes, including technical changes. We propose that the provision would require the notification to be made a reasonable time before relevant changes are implemented."*

12. The relationship between this obligation and Technical Capability Notices (TCNs) is not explicitly set out.

13. Taken together, these proposals appear to create new legal mechanisms for the Home Office to be able to halt a platform from upgrading its structural systems, for example, by introducing end-to-end encryption across its service. The powers could be used to prevent such a course of action entirely under the threat of a TCN.

14. Using these mechanisms to prevent a company from introducing end-to-end encryption across its service would have a direct baring on enjoyment of the right to privacy and would be entirely disproportionate given the powers the Home Office and Security services have to access information at device level or even compromise end-to-end encryption through existing powers.

15. As the former UN Special Rapporteur on Freedom of Expression observed in a report on encryption and anonymity, in 2015:

> *"States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows."*[5]

16. This technology provides immense benefits in keeping people safe and secure in the UK and around the world and the consequences of preventing a service from deploying end-to-end encryption should also be taken into consideration. End-to-end encryption is a particularly vital protection for human rights defenders and journalists who rely on private messaging to do their jobs in hostile environments; and for those who depend on privacy to be able to express themselves freely, like LGBTQ+ people.

5 Kaye, D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, GE. 15-07497, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

17. These proposals should also be considered alongside new powers to compel service providers to use "accredited technology" under the Online Safety Bill[6]. These powers in the Bill are themselves entirely disproportionate and could compel a company to deploy technology known as "client-side scanning" across an entire messaging platform. This kind of mass monitoring undermines the principle that suspicion should preceed surveillance and could open individuals up to having their devices compromised by a range of actors, including high-profile individuals who rely on encrypted messaging services for their own privacy.

18. The consequence of these proposals set by the Home Office and those in the Online Safety Bill will be the possibility that major communications services could leave the UK market or offer a reduced service. This has been threatened by private messaging service, Signal in response to the Online Safety Bill[7] and Apple in response to the Home Office's proposals set out in this consultation[8]. WhatsApp have also stated they will not comply with proposals in the OSB that would cause them to weaken their security[9] which could cause the service to be blocked in the UK under powers in the legislation[10]. This does not take into account the raft of smaller services that may choose not to operate in the UK on account of both legislative proposals.

19. A reluctance to operate in the UK or an exodus from the UK market by major service operators such as Signal and WhatsApp would seriously damage freedom of expression in Britain, restricting the public's ability to freely communicate with people in other jurisdictions. Such a scenario would not only put British citizens and businesses at a global disadvantage but would place them at greater risk through having to resort to communications providers with poor security practices.

CONCLUSION

20. The proposals regarding revised notices regimes under the Investigatory Powers Act 2016 raise a number of concerns regarding their impact on the rights to freedom of expression and privacy.

6 See clause 122, Notices to deal with terrorism content or CSEA content (or both), Online Safety Bill, https://bills.parliament.uk/publications/52368/documents/3841

7 Signal app warns it will quit UK if law weakens end-to-end encryption, Guardian Online, 24 Februrary 2023, https://www.theguardian.com/technology/2023/feb/24/signal-app-warns-it-will-quit-uk-if-law-weakens-end-to-end-encryption

8 Apple slams UK surveillance-bill proposals, BBC News Online, 21 July 2023, https://www.bbc.co.uk/news/technology-66256081

9 WhatsApp would not remove end-to-end encryption for UK law, says chief, Guardian Online, 9 March 2023, https://www.theguardian.com/technology/2023/mar/09/whatsapp-end-to-end-encryption-online-safety-bill

10 See clause 145, Service restriction orders, Online Safety Bill, https://bills.parliament.uk/publications/52368/documents/3841

21. Taken together, these proposals present as a new legal framework to halt or even prevent companies from rolling out security measures, such as end-to-end encryption, across their services.

22. Given the powers available to the Home Office and UK-wide security services to circumvent end-to-end encryption, these powers are neither necessary nor proportionate. In particular, proposals which would require companies to notify the Home Office of any technical changes to their service should be dropped.