WRITTEN EVIDENCE FROM FREEDOM FROM OPEN RIGHTS GROUP (IPA0007)

Does the introduction of a notification requirement requiring operators to inform the Secretary of State if they propose to make changes to their products or services that would negatively impact existing lawful access capabilities raise any human rights concerns?

The objective of this notification requirement appears designed to impose a "freeze" on changes to the service while consultations are taking place. The intention appears to stop user security improvements from being rolled out.

While this objective may appear reasonable, it would allow the Secretary of State to prevent secure services from launching in the UK, even where they are deployed elsewhere. This provision would allow the Secretary of State and the Home Office to place itself in a position of power over the provider as soon as it hears about updates that might make data less accessible than it is currently. This situation would take place without reference to an independent authority to assess the rationale or proportionality. Such a move might not be proportionate, for instance, if the security technology had already been introduced safely and with demonstrable benefits to users in other parts of the world.

Open Rights Group is concerned these powers could deny people access to technological developments upon which people's free expression and right to privacy rely. For example, major tech providers such as Apple have stated that they would pull certain services from the UK rather than compromise their security if this power was used to prevent them from rolling out security updates[1].

Our main concerns in the proposed revisions relate to weakened privacy and expanded government surveillance. Under the new proposals, the UK government could prevent a communications services provider from fixing software vulnerabilities through essential security updates[2] or applying advanced protections such as end-to-end encryption to their services at a global level. Requiring prior approval before rolling out a security patch is not a proportionate response.

ORG is also concerned that the changes are meant to reduce the possibility of the introduction of encryption to protect user data from unwanted access.

The Home Office appears to regard encryption, especially "end-to-end encryption" (E2EE), where a service provider is unable to see the contents of communications they facilitate, as a threat to its capabilities and, by extension, to national security. It appears to be seeking to extend its powers to prevent E2EE from being used at scale, despite its benefits to users and vendors.

E2EE is a significant protection for the right to privacy against everyday criminality, abuse and intrusion. Encrypted messaging apps are routinely used by politicians, doctors, lawyers, and others who need to exchange large amounts of personal data securely while complying with UK data protection legislation.

---

1. [1]Apple slams UK surveillance-bill proposals https://www.bbc.co.uk/news/technology-66256081
2. [2]Changes to UK Surveillance Regime May Violate International Law https://www.justsecurity.org/87615/changes-to-uk-surveillance-regime-may-violate-international-law/

Journalists rely on E2EE and access to secure global technologies to communicate with their sources and exercise freedom of expression rights. E2EE protects vendors from being a vector for potentially massive data loss.

In addition, the proposed measures in The Investigatory Powers (Amendment) Bill are poised to profoundly impact political dissidents and opposition figures residing in the UK. Refugees, political exiles, and human rights advocates who have sought refuge within the UK deserve the assurance of digital safety and security.

LGBTQ+ individuals from refugee and migrant backgrounds who have fled to the UK heavily rely on digital tools to maintain connections with their families, friends, and social networks. These individuals will face heightened vulnerabilities to hacking and privacy breaches if the proposed changes are implemented.

Undermining security updates and patches is especially concerning for exiled activists who have been compelled to leave their home countries and now reside in the UK. These individuals may become susceptible to digital transnational repression attacks from their authoritarian regimes. Such attacks, coupled with a sense of deprivation of digital safety and security, will inevitably lead to severe consequences on their freedom of expression, potentially resulting in silencing their voices.

The exiled diaspora from countries such as Iran, Saudi Arabia, and Hong Kong has historically faced harassment and digital threats from their authoritarian regimes, even beyond their national borders. The proposed measures in the Bill could significantly exacerbate this situation, providing authoritarian governments with unprecedented opportunities to control, silence, and punish dissent across borders[3]. Forensic Architecture, a London-based research agency, has documented 326 incidents of digital transnational repression between 2019 and 2021[4]. This number is likely to rise, especially in cases where security updates for technology are undermined. Numerous refugees and diaspora from Hong Kong, along with prominent activists, have expressed feelings of insecurity following online threats and harassment in the UK from their government [5].

Additionally, three UK-based civil society leaders and human rights activists have reported their mobile devices being infiltrated with spyware by their regimes[6]. These examples underscore the urgent need to reconsider the potential ramifications of the proposed amendments and their impact on the safety and security of those who seek refuge and advocate for justice within the UK.

While the government may have particular reasons to seek access to data and systems in certain

[3]The Digital Transnational Repression Toolkit, and Its Silencing Effects https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-its silencing-effects -

[4] Digital repression across borders is on the rise https://www.technologyreview.com/2022/07/08/1055582/digital-repression-across-borders-is-on-the-rise/ -

[5] 'We don't feel safe here': Hongkongers in UK fear long reach of Chinese government- https://www.theguardian.com/global-development/2023/oct/17/we-dont-feel-safe-here-hongkongers-in-uk-fear-long-reach-of-chinese-government -

[6] Bindmans launches legal action in the United Kingdom on misuse of Pegasus spyware- https://www.bindmans.com/knowledge-hub/news/bindmans-launches-legal-action-in-the-united-kingdom-on-misuse-of-pegasus-spyware/ -

limited circumstances, it should neither assume that all data should be easily accessible nor seek legal regimes to ensure that data is kept easily accessible.

We reiterate that encryption does not prevent lawful access per se. It may require law enforcement to access a device covertly or to seize it and demand passwords; however, these approaches are likely to be more proportionate than simply preventing security measures from evolving for the population at large.

Instead of preventing improved technological security features upon which people's right to free expression and right to privacy rely for the population at large, the Home Office should instead seek to use more proportionate investigative methods that do not infringe upon people's human rights.

Do any of the changes made by the Bill mean that journalists, journalistic sources or journalistic material can be interfered with in breach of Article 10 ECHR? Does the Bill contain sufficient safeguards to prevent breaches?

Information Security is essential for journalists who need to protect their work and sources[7]. Any attempts to delay or halt security updates or improvements to software could have an adverse impact on journalists by making them more susceptible to attacks from hostile actors or foreign states, as we saw occur with the Pegasus scandal[8].

This could have particular impact on journalists in the UK, who could find their communications with sources restricted if tech providers were prevented from deploying software already adopted by sources or journalists in other countries.

Are the provisions expanding access to Internet Connection Records compatible with Article 8 ECHR? Do the provisions contain sufficient safeguards to ensure compatibility?

No. Our own legal challenge at the CJEU, as a party to the Watson case[9], enforcing similar rights, showed that he court understood the sensitivity of this data. We are particularly concerned that Clause 14 expands the use of Internet Connection records, essentially for Pre-Crime target detection, or "network analysis". There is considerable scope for fishing expeditions, targeting of people for associations, and other practices which are neither wise nor proportionate.

---

[7]Why journalism needs information security
https://reutersinstitute.politics.ox.ac.uk/calendar/why-journalism-needs-information-security
[8]Pegasus scandal: Are we all becoming unknowing spies?
https://www.bbc.co.uk/news/technology-57910355
[9]Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others.https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62015CJ0203

The appropriate safeguard with most data surveillance is to notify those involved where it is safe to do so. The UK government was asked for this change in the Watson case, but it was not implemented. Such a change would allow people who had been surveilled for bad reasons to challenge the abuse of their privacy. Without the knowledge that surveillance has taken place, anticipating the need to challenge is extremely hard. Notification is an evolving requirement but an obvious one where capabilities inevitably grow with technology.

About Open Rights Group (ORG): Founded in 2005, Open Rights Group (ORG) is a UK-based digital campaigning organisation working to protect individuals' rights to privacy and free speech online. ORG has been following the UK government's proposed changes to the Investigatory Power Act since their inception. In November 2023, we wrote a **thorough response** to UK government's consultation on the amendments.

Imprint: Published by Open Rights, a non-profit company limited by Guarantee, registered in England and Wales no. 05581537. The Society of Authors, 24 Bedford Row, London, WC1R 4EH.

(17 January 2024)