February 21, 2025

The Rt Hon Yvonne Cooper
Secretary of State for the Home Department
2 Marsham Street
London
SW1P 4DF4

The Rt Hon Sir Brian Leveson
Investigatory Powers Commissioner's Office
PO Box 29105
London
SW1V 1ZU

Re: UK demands access to encrypted data worldwide

Dear Home Secretary and Sir Brian,

We are civil society groups, scholars of fundamental rights law, and computer security experts concerned about communications security and cybersecurity implications of compromising end-to-end encryption. We write to urge the United Kingdom to uphold fundamental rights by withdrawing its secret demands to Apple that imperil strong encryption. Encryption technologies, the European Court of Human Rights (ECtHR) has recognized, "contribute to ensuring the enjoyment of fundamental rights, such as freedom of expression," and "help citizens and businesses to defend themselves against abuses of information technologies, such as hacking, identity and personal data theft, fraud and the improper disclosure of confidential information."[1] The Court cited the United Nations High Commissioner for Human Rights's 2022 Report on the Right to Privacy in the Digital Age: "Encryption is a key enabler of privacy and security online and is essential for safeguarding rights … . Encryption ensures that people can share information freely, without fear that their information may become known to others, be they State authorities or cybercriminals."[2]

Despite Brexit, the United Kingdom remains bound by the European Court of Human Rights' interpretation of the European Convention on Human Rights, to which the UK and 45 other European countries are signatories. Yet your government is violating the Convention and fundamental precepts of human rights law by trying to break secure encryption. "Technical capability notices" sent by the Home Office to Apple in January 2025 pursuant to the Investigatory Powers Act of 2016 reportedly demand access to "all the content any Apple user worldwide has

[1] Podchasov v. Russia, no. 33696/19, § 76, ECHR 2024, 13 February 2024.
[2] Ibid. § 28 (quoting *Report On The Right To Privacy In The Digital Age*, Office of the United Nations High Commissioner for Human Rights, § 21, 4 August 2022 (A/HRC/51/17) (*2022 Report*)), https://digitallibrary.un.org/record/3985679?ln=en&v=pdf).

uploaded to the cloud."[3] This demand has "no known precedent in major democracies."[4] It compels Apple to decrypt, and allow the U.K. access to, user data currently protected by end-to-end encryption (E2EE), the best available technology for protecting stored messages, documents, and other material. Your notices require immediate compliance even pending an appeal through a process that is—like the notices—secret by law. If your government denies the appeal and insists on enforcing its demands, they will undoubtedly be challenged on behalf of affected users at the ECtHR.

There is no realistic prospect that the Court will uphold these demands. Notably, when the Court upheld a law requiring the identification of users (registration of SIM cards), it did so only because the law did "not extend to … data which reveal the content of communication"[5]—precisely what your notice demands access to. As the Court has noted (again quoting the 2022 High Commissioner's report), "the impact of most encryption restrictions on the right to privacy and associated rights are disproportionate, often affecting not only the targeted individuals but the general population. Outright bans by Governments … cannot be justified as they would prevent all users within their jurisdictions from having a secure way to communicate."[6] Just so here: your demand amounts to an outright ban that would affect all users, not merely alleged criminals, and thus cannot be justified. Worse, you have demanded that Apple make such changes not only for users within the UK but worldwide; the global scope of this demand makes it even less likely to be upheld by the ECtHR.

Your demand is not proportionate to any legitimate interest because it imposes significant risks on users: Your notices amount to precisely what the High Commissioner warned against: "a blanket restriction of encryption that could require, or at least encourage, the creation of some sort of back door (a built-in path to bypass encryption, allowing for covert access to data in plain text)."[7]

---

[3] Joseph Menn, *U.K. orders Apple to let it spy on users' encrypted accounts*, Wash. Post (Feb. 7, 2025), https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/. Because these notices are required to be secret, similar demands may also have been made to other companies, but we would have no way of knowing until they were leaked to the press. Apple's Advanced Data Protection is optional for iCloud users.

[4] *Id.*

[5] Breyer v. Germany, no. 50001/12, § 61, 30 January 2020.

[6] Podchasov § 28, https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-230854%22]}.

[7] *2022 Report* § 23.

This would "jeopardize the privacy and security of all users and expose them to unlawful interference, not only by States, but also by non-State actors, including criminal networks."[8]

To comply, Apple must either build a backdoor into its end-to-end encrypted cloud service (which could, and would, then be accessed by malicious actors) or cease offering E2EE cloud services altogether. The "adverse effects" of restricting E2EE, warned the High Commissioner, "are not necessarily limited to the jurisdiction imposing the restriction; rather it is likely that back doors, once established in the jurisdiction of one State, will become part of the software used in other parts of the world."[9] Apple is right: no single government should "have the authority to decide for citizens of the world whether they can avail themselves of the proven security benefits that flow from end-to-end encryption."[10] Denying the benefits of encryption to users everywhere is wildly disproportionate to any legitimate interest your government may have.

We urge you to withdraw the TCNs to Apple immediately.

Sincerely,

Civil Society Organizations

TechFreedom
Advocacy for Principled Action In Government
Center for Democracy & Technology
Competitive Enterprise Institute
Freedom of the Press Foundation
Information Technology and Innovation Foundation
New America's Open Technology Institute
R Street Institute
The Future of Free Speech

Academics & Computer Scientists[11]

Neil Chilson
Head of AI Policy
Abundance Institute

Brian L. Frye
Spears-Gilbert Professor of Law
University of Kentucky College of Law

Jess Miers
Visiting Assistant Professor of Law
University of Akron School of Law

Riana Pfefferkorn
Policy Fellow
Stanford HAI

[8] *Id.* § 25. *See also* Fed. Commc'ns Comm., Fact Sheet: Implications of Salt Typhoon Attack and FCC Response (Dec. 5, 2024), https://docs.fcc.gov/public/attachments/DOC-408015A1.pdf.
[9] *Id.*
[10] Written Evidence, Apple Inc., on the Investigatory Powers Bill, IPAB10 (2024), https://publications.parliament.uk/pa/cm5804/cmpublic/InvestigatoryPowersAmendment/memo/IPAB10.htm.
[11] Individual signatories' affiliations are shown for purposes of identification only.