13 March 2025

To: The Rt Hon Lord Justice Singh
President, Investigatory Powers Tribunal

cc: Mr Justice Johnson

Dear Lord Justice Singh,

As organisations committed to defending privacy and freedom of expression rights, we are writing in response to reports that the Investigatory Powers Tribunal ('IPT') will be hearing Apple's appeal against a Home Office Technical Capability Notice ('TCN') issued under the Investigatory Powers Act 2016 (the 'IPA') this Friday, 14 March 2025. Although the IPT can choose whether to hold hearings and whether to hold them in public or private, we invite you to make this process more transparent by opening this hearing to the public.

Our organisations have long been involved in surveillance issues in the UK and abroad, including in cases started at or ruled on by the IPT. Open Rights Group and Big Brother Watch originated complaints that led to the judgment in *Big Brother Watch and others v UK*,[1] in which the Court ruled that the UK's bulk interception powers under the Regulation of Investigatory Powers Act 2000, predecessor to the IPA, were in

[1] App Nos 58170/13, 62322/14 and 24960/15, 25 May 2021 (GC)

breach of Article 8 of the ECHR. Our organisations submitted a joint briefing to the House of Lords on the Investigatory Powers (Amendment) Bill in January 2024, notably expressing concerns at the time on the interdiction on recipients of TCNs to disclose their existence or contents. Index on Censorship has more recently been involved in encryption-related debates due to the growing threats to freedom of expression posed by policies such as those introduced by the Online Safety Act 2023[2] and Ofcom's characterisation of encryption as a risk factor in its guidance on illegal harms measures.[3]

This case implicates the privacy rights of millions of British citizens who use Apple's technology, as well as Apple's international users. There is significant public interest in knowing when and on what basis the UK government believes that it can compel a private company to undermine the privacy and security of its customers. There are no good reasons to keep this hearing entirely private, not least for the fact that the existence of the TCN has already been widely reported and that Apple's own actions in removing its Advanced Data Protection (ADP) feature for UK iCloud users[4] leave no doubt as to what triggered them – despite reports that the government considers this removal does not comply with the TCN.[5]

According to reporting across the globe, the Secretary of State for the Home Department has issued Apple with a TCN under the Investigatory Powers Act,

---

[2] https://www.indexoncensorship.org/2022/05/online-safety-bill-will-significantly-curtail-freedom-of-expression/
[3] https://www.indexoncensorship.org/2024/12/media-regulator-fails-to-properly-protect-freedom-of-expression-in-online-safety-draft-guidance/
[4] https://support.apple.com/en-gb/122234
[5] Financial Times, Apple launches legal challenge to UK 'back door' order, 4 March 2025: https://www.ft.com/content/3d8fe709-f17a-44a6-97ae-f1bbe6d0dccd

requiring the company to create a technical capability enabling access to end-to-end encrypted data on its iCloud service if requested by the UK Government.[6] End-to-end encryption cannot be broken in a targeted manner – once a 'backdoor' into the system has been created, it can be exploited by anyone, putting the privacy and security of all users at risk.

International human rights treaty bodies have recognised the importance of end-to-end encryption to protect the right to privacy and to promote the exercise of other rights. This is because safe and secure communications can be a precondition of being able to express one's views, seek help and protection, share vital information, or avoid censorship.

The case law of the European Court of Human Rights (ECtHR), for example, recognises the role of anonymity in "promoting the free flow of ideas and information in an important manner" including by protecting people from reprisals for their exercise of freedom of expression.[7] The ECtHR has also recently recognised that the very threat or potential of an obligation to decrypt communications constituted an interference with Article 8 rights,[8] and that undermining end-to-end encryption impacts the rights of all users to defend themselves against various threats and to exercise various freedoms.[9] It therefore found that an "obligation to decrypt end-to-end encrypted communications risks amounting to a requirement that providers of such

---

[6]U.K. orders Apple to let it spy on users' encrypted accounts – Joseph Menn, the Washington Post, 7 February 2025: https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/ ; Apple pulls data protection tool after UK government security row – BBC News, 22 February 2025: https://www.bbc.co.uk/news/articles/cgj54eq4vejo

[7]*Delfi AS v Estonia* [2015] EMLR 26, [147] and [149]

[8] *Podchasov v Russia* [2024] ECHR 134, [58]

[9] Ibid, [76]

services weaken the encryption mechanism for all users; it is accordingly not proportionate to the legitimate aims pursued".[10]

The IPT is required to hold hearings in public, unless doing so would threaten the public interest or prejudice national security.[11] All Apple iCloud users in the UK who had turned on ADP are already suffering the consequences of Apple's decision to withdraw the protection in the country, and fully aware of the reasons for this decision. It is not conceivable that a confirmation of the *existence* of the TCN would threaten the UK's interests to a level or in a form that meets the conditions for derogating from the principles of open justice. The principles that have in the past allowed the UK government to maintain an NCND policy are only relevant to the targeted interception of communications and covert surveillance.[12] They cannot apply to such a wide and already public piece of information about the UK's attempts to weaken the security of services used by millions of people in and outside the UK. The IPT itself has recognised its function as a judicial body to determine whether secrecy measures are strictly necessary and proportionate to the objectives of an NCND policy.[13] We invite you to exercise this function with rigour and in the light of the requirements of open justice.

Further, hearings in private must be strictly confined to matters that are prejudicial to the interests mentioned in Rule 7(1) of the Tribunal Rules. As the IPT recognised in its *Kennedy* ruling, *"purely legal arguments, conducted for the sole*

---

[10] Ibid, [79]

[11] Tribunal Rules – The Investigatory Powers Tribunal website, accessed 12 March 2025: https://investigatorypowerstribunal.org.uk/tribunal-rules ; The Investigatory Powers Tribunal Rules 2018, Rules 10 and 7(1)

[12] Kennedy *and Other* [2003] IPT/01/62 and IPT/01/77, [46]

[13] Ibid, [58]

purpose of ascertaining what is the law and not involving the risk of disclosure of any sensitive information, should be heard in public. The public, as well as the parties, has a right to know that there is a dispute about the interpretation and validity of the relevant law and what the rival legal contentions are."[14] We urge you to ensure that holding all or part of Friday's hearing in private does not derogate from this ruling.

The public interest lies in conducting this hearing in public. There is significant public interest in the matter, evident in the extensive and ongoing media reporting on it, and in the impact it will have on the rights of users of lawful services across the globe. We invite you to provide the requisite level of transparency and scrutiny over an already widely reported situation.

Yours sincerely,

Jim Killock,
Executive Director, Open Rights Group

Jemimah Steinfeld,
Chief Executive Officer, Index on Censorship

Rebecca Vincent,
Interim Director, Big Brother Watch

[14] Ibid, [172]