# UK drops demand for Apple backdoor after talks with US, spy chief says



Washington/London — Britain has dropped its demand for Apple to provide a backdoor that would have allowed access to encrypted data stored by U.S. users, DNI Tulsi Gabbard said on X on Monday. The claim comes after months of high‑level talks that reportedly involved Washington and London, with President Donald Trump and Vice‑President JD Vance named as participants in the effort. According to the original report, British Prime Minister Keir Starmer was in Washington that day to meet Trump and other European leaders to discuss Russia’s war in Ukraine. A British government spokesperson declined to comment on any agreement but stressed that London has long worked with the United States to tackle security threats while protecting the privacy of citizens. Apple did not respond to requests for comment. The background matters: Apple had withdrawn its Advanced Data Protection feature for UK users in February after a UK order seeking backdoor access under the Investigatory Powers Act. Apple has said it would never build such access, while cybersecurity experts warned that any backdoor could be discovered and misused. The company’s position and the security implications have been a persistent point of contention in the cross‑border data dialogue.

The dispute centred on whether UK authorities could compel access to encrypted data in Apple’s iCloud backups and other services under the Investigatory Powers Act or the CLOUD Act, and what that would mean for privacy and security in both countries. Reuters summaries of the U.S. assessment note that officials were examining whether Britain had violated bilateral data‑sharing frameworks by pressing for such access. In addition, observers highlighted that Apple had already removed ADP for UK users in February, a move that underscored the practical consequences of the case for data protection in Britain. The Guardian’s reporting later explained that Apple’s ADP removal shifted more data to standard encryption, which Apple could access with warrants, raising questions about what data remains protected by default encryption and what that implies for cross‑border investigations.

BBC News’s coverage provides a country‑level technical snapshot: Apple’s ADP tool in Britain was no longer offered to new UK customers, with the nine data categories previously covered by ADP reclassified under Standard Data Protection, while 14 categories remained end‑to‑end encrypted by default. iMessage and FaceTime remain protected by end‑to‑end encryption. The Home Office was described as seeking access under the Investigatory Powers Act, a framing that has fuelled ongoing debate about privacy, civil liberties and the handling of cross‑border data. The Guardian’s August coverage adds that officials did not publicly confirm any agreement and emphasises the diplomatic sensitivities surrounding intelligence sharing, with privacy advocates warning that any erosion of encryption standards could have broader security implications.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://www.staradvertiser.com/2025/08/19/breaking-news/tulsi-gabbard-says-u-k-drops-apple-backdoor-mandate/), [[4]](https://support.apple.com/en-mide/122234)
* Paragraph 2 – [[1]](https://www.staradvertiser.com/2025/08/19/breaking-news/tulsi-gabbard-says-u-k-drops-apple-backdoor-mandate/), [[2]](https://www.reuters.com/sustainability/boards-policy-regulation/us-spy-chief-gabbard-says-uk-agreed-drop-backdoor-mandate-apple-2025-08-19/), [[5]](https://www.theguardian.com/technology/2025/feb/21/apple-removes-advanced-data-protection-tool-uk-government)
* Paragraph 3 – [[3]](https://www.bbc.co.uk/news/articles/cgj54eq4vejo), [[6]](https://www.theguardian.com/technology/2025/aug/19/uk-has-backed-down-on-demand-to-access-us-apple-user-data-spy-chief-says)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.staradvertiser.com/2025/08/19/breaking-news/tulsi-gabbard-says-u-k-drops-apple-backdoor-mandate/> - Please view link - unable to able to access data
2. <https://www.reuters.com/sustainability/boards-policy-regulation/us-spy-chief-gabbard-says-uk-agreed-drop-backdoor-mandate-apple-2025-08-19/> - US Director of National Intelligence Tulsi Gabbard claimed that the United Kingdom had agreed to drop its backdoor mandate on Apple after months of negotiations. In a post on X, she described a deal involving Britain, the United States, President Trump and Vice President Vance, intended to balance privacy with security cooperation. Reuters notes the dispute centred on access to encrypted data held in iCloud backups and other Apple services, and on whether UK authorities could compel such access under IPA or CLOUD Act frameworks. The report recalls Apple’s removal of ADP for UK users earlier in 2025 and the ongoing cross‑border data‑access scrutiny, underscoring tensions between encryption, privacy and security.
3. <https://www.bbc.co.uk/news/articles/cgj54eq4vejo> - BBC News reports that Apple removed its Advanced Data Protection feature for UK customers following a government security row. ADP provided end-to-end encryption so only users could access certain iCloud data, while Apple argued it could not access the data itself. The Home Office was described as seeking backdoor access under the Investigatory Powers Act, prompting Apple to disable ADP for new UK users and plan a later disablement for existing users. The piece notes that other data remains protected by default encryption and includes expert commentary on privacy, civil liberties and potential impacts on international data‑sharing norms.
4. <https://support.apple.com/en-mide/122234> - Apple confirms in its official support page that the United Kingdom will no longer be offered Advanced Data Protection to new users. The change means nine iCloud data categories previously covered by ADP move to Standard Data Protection, while 14 iCloud data categories remain end-to-end encrypted by default. The page states that iMessage and FaceTime continue to be end‑to‑end encrypted. It also explains that UK users who already had ADP enabled will be given a grace period to disable the feature themselves, with no automatic deactivation by Apple. ADP remains available in other regions.
5. <https://www.theguardian.com/technology/2025/feb/21/apple-removes-advanced-data-protection-tool-uk-government> - The Guardian reports that Apple withdrew its Advanced Data Protection for UK customers after a government request for access to encrypted data under the Investigatory Powers Act. Apple reiterated that it has never built a backdoor. The article notes ADP as the most protective encryption option and explains that its removal shifts more data to standard encryption, potentially readable by Apple with warrants. It features expert commentary warning that any backdoor could undermine security and privacy beyond the UK and discusses the regulatory controversy surrounding cross‑border data access.
6. <https://www.theguardian.com/technology/2025/aug/19/uk-has-backed-down-on-demand-to-access-us-apple-user-data-spy-chief-says> - The Guardian covers Tulsi Gabbard’s claim that the UK reversed its demand to access encrypted Apple data following sustained U.S. pressure. The article notes that officials did not publicly confirm an agreement and that operational details remained unconfirmed. It outlines the legal framework around cross‑border data access, IPA and CLOUD Act, and highlights privacy advocates’ warnings about weakening encryption. The piece emphasises the diplomatic sensitivities of the dispute and the potential implications for intelligence sharing between the United States and the United Kingdom.
7. <https://www.theregister.com/2025/02/24/rather_than_add_a_backdoor/> - The Register reports that Apple chose to end iCloud Advanced Data Protection for UK users in response to government pressure. It explains that the UK order would have granted access to backups and related data, and discusses the security implications of removing ADP, including the possibility that data could be read by Apple under legal warrants. The piece frames the broader debate around encryption, backdoors and privacy, contrasting regulatory efforts to improve law enforcement access with the risk of creating systemic vulnerabilities that could be exploited.