CS7NS5: Security & Privacy Assignment 2

Cormac Sharkey
20333458

March 2025

Apple vs. UK Government: Data privacy

Earlier this year, Apple received a confidential request from the UK government [1, 2] for access to their users' data, through the Home Office under the Investigatory Powers Act, or IPA. The IPA gives UK law enforcement powers to request and obtain information from companies, including user data. The request targets Apple's Advanced Data Protection feature, or ADP, which allows its users to enable end-to-end encryption on messages and cloud data. This level of security hides a user's data from everyone, even Apple themselves.

The request, while it cannot be publicly disclosed due to its ties to the IPA, is likely motivated to allow for targeting of terrorist activity and/or criminal activity involving personal data. Apple have previously refused requests by law enforcement to access their devices and stored data, despite circumstances linking users of their devices to criminal activity. In the past, Apple's refusal has led to law enforcement turning to outside parties to unlock devices, such as iPhones, to gain access to sensitive information in an attempt to investigate terrorism. However, due to the incredibly secure nature of ADP, no third party would have the capabilities to access data encrypted under it, nor would Apple, as previously mentioned.

The request requires Apple to add a backdoor to this feature, effectively breaking end-to-end encryption for anyone who knows how to get in. This would allow Apple and, by extension, UK law enforcement to have access to data encrypted under ADP. Apple, alongside the security and privacy community as a whole, are against adding backdoors into security systems and devices, for fear bad actors with malicious intent could find their way inside to steal all Apple user data. In response, Apple blocked ADP from being newly enabled in the UK [3], leaving existing users of the feature with access until an unspecified future data. This was an attempt to appease the UK government, however, it is most likely not enough to satisfy the request.

An event like this is highly significant, not only for the entirety of the UK, but also for the world. A government body making a direct request for unfiltered access to user data sets a horrifying security and privacy precedent. A success for the UK government would open the doors for any other nation, whether good-intentioned or otherwise, to do the same. If Apple loses this fight and are forced into adding a backdoor or permanently disabling ADP, it will give other governments or bodies of power the courage to do the same, regardless of their goals. Requesting access to private company data, that is, user data, would become a dangerous norm around the world.

Events like these are the exact reason why security standardisations are crucial for the protection of human rights, such as privacy. If end-to-end encryption with no backdoors was a standard for companies dealing with personal communications and data, this request would almost certainly have never become a legitimate threat to user security and privacy. To take an example, the internet features many security protocols for communication that all service providers must comply with to maintain access. If a government body were to demand a particular provider to disable these security protocols for their services, they would immediately break and become non-functional, because they are no longer following the same standards as everyone else. But as Apple's ADP is not standard and can be disabled without functionality-related ramifications, it becomes an exposed flaw that can be undone by forceful laws.

Fortunately, Apple understand the impact this can have on global privacy and security, as they are a strong advocate for user data protection. Most recently, they have taken legal action against the UK government to appeal this request [4], hoping to revoke the demand to install a backdoor into the ADP system. If Apple's attempt at legal action is successful, their end-to-end encryption system will remain intact and Apple user's will be able to retain their data privacy. If not, it is likely to cause upset among the security and privacy community, as Apple will surely have to add a backdoor into ADP, or remove it as a feature entirely.

References

[1] Joseph Menn. U.K. orders Apple to let it spy on users' encrypted accounts. *The Washington Post*, February 2025. ISSN 0190-8286. URL https://www.washingtonpost.com/technology/2025/02/07/apple-encryption-backdoor-uk/.

[2] Zoe Kleinman. UK government demands access to Apple users' encrypted data, February 2025. URL https://www.bbc.com/news/articles/c20g288yldko.

[3] Zoe Kleinman. Apple pulls data protection tool after UK government security row, February 2025. URL https://www.bbc.com/news/articles/cgj54eq4vejo.

[4] Zoe Kleinman. Apple takes legal action in UK data privacy row, March 2025. URL https://www.bbc.com/news/articles/c8rkpv50x01o.