The UK will neither confirm nor deny that it’s killing encryption



The United Kingdom dealt a significant blow in its war on encryption last week that, aside from blemishing Apple’s meticulously curated privacy commitments, could have worldwide ramifications for personal data protections. And while several days have passed since Apple pulled its Advanced Data Protection (ADP) feature from UK customers, other end-to-end encryption providers like Meta, Signal, and Telegram have yet to meaningfully take an official stand beyond some of their execs posting about it on social media.

The UK may have set a precedent for other global governments to follow when it reportedly ordered Apple to give it backdoor access to iCloud data. Under the 2016 Investigatory Powers Act (IPA), the British government can legally demand user data be

handed over for the purpose of national security and crime prevention. That seemingly includes *worldwide* data access, even if it's tightly encrypted.

Some of these demands would be facilitated by controversial changes that were made to the IPA in April 2024 to expand its surveillance capabilities, like allowing intelligence services to access bulk personal datasets held by third parties and the UK government to interfere with communications companies that want to offer encryption services.

We don't know specifically how the UK's order was worded. *The Washington Post* reported that Apple received a "technical capability notice" under the IPA that demanded it create a "backdoor" to its iCloud service that provides "blanket capability to view fully encrypted material, not merely assistance in cracking a specific account."

This may be an interpretation of the order. According to Home Office state minister Dan Jarvis, a technical capability notice itself does not require specific information to be disclosed. Instead, it forces companies "to have the capability to respond to an individual warrant or authorisation." In other words, it prevents operators from having technology in place – such as full encryption services with user-only access – that could block the UK from snooping when it chooses to.

The order given to Apple is believed to be the first such demand made since the IPA was updated last year. We don't really know if other companies have been slapped with similar orders because it's illegal to publicly acknowledge if they've received one. Britain insidiously designed its war against data encryption to happen almost entirely behind locked doors. Apple can appeal the ruling in secret but can't reveal if it exists. It can't even say if it's complying. The only reason we know about the order is because it was leaked to *The Washington Post.*

We don’t really know if other companies have been slapped with similar orders because it’s illegal to publicly acknowledge if they’ve received one

The British Home Office department also won’t confirm or deny its involvement. The statement it gave to *The Verge* said, “We do not comment on operational matters, including for example confirming or denying the existence of any such notices.”

Instead, the Cupertino, California-based company pulled its highest-level data security tool from the country without explanation after *The Washington Post* article was published. The ADP feature expands the end-to-end encryption provided on passwords, health data, and payment information to include iCloud drives and backups, Notes, Photos, Voice memos, and more.

“The UK government put Apple in an untenable position by demanding a backdoor in end-to-end encryption in iCloud for users everywhere in the world,” Andrew Crocker, surveillance litigation director at the Electronic Frontier Foundation (EFF), told *The Verge*. “Apple’s decision to disable the feature for UK users could well be the only reasonable response at this point, but it leaves those people at the mercy of bad actors and deprives them of a key privacy-preserving technology.”

Given the UK reportedly demanded *global* access to data, it’s unclear if withdrawing ADP from the country has appeased the order. It will, however, remove some obstacles that prevent the UK government from spying on its own citizens, which, as Crocker notes, makes people “less safe” from potential security threats and “less free.” Apple had already threatened to withdraw security features from the UK market when it opposed the IPA bill, but the decision to do so still attracted criticism for clashing with the image it’s built around being a self-professed defender of privacy rights.

Apple’s withdrawal of ADP can be interpreted as a call to break an intentionally curated silence around Britain’s bullish efforts to crush end-to-end encryption services. It’s a call that other encryption service providers don’t seem to be answering, however. Meta, Signal, and Telegram haven’t made any announcements about their own services that provide full encryption and haven’t responded to our requests to comment on the situation. Their silence and the ongoing availability of encryption features in the UK would suggest that nothing is amiss.

Thorin Klosowski, a security and privacy activist at the EFF, says that this is likely the case because the encryption services provided by most communications companies aren’t as broad as Apple’s ADP offering.

“Few companies offer anything exactly like Advanced Data Protection, and as it stands, Apple is saying it believes it can still offer the end-to-end encryption of iMessage,” Klosowski told *The Verge*. “If history is any indication, if the end-to-end encryption of the other communication apps, like Signal or WhatsApp, was targeted, those companies would make noise about it.”

“Few companies offer anything exactly like Advanced Data Protection”

WhatsApp and Signal have both previously threatened to leave the UK if their services were forced to weaken encryption standards under the country’s Online Safety Bill. WhatsApp chief Will Cathcart has also commented on the UK versus Apple situation directly on social media, but neither WhatsApp nor its parent company, Meta, has provided an official statement.

“Encryption is absolutely critical for keeping people safe, and governments should encourage it,” Cathcart said on X. “Banning encryption is a dangerous gift to hackers and hostile foreign governments.”

Most of the outcry hasn’t been from at-risk companies but, rather, from privacy rights groups and government officials. The US is also investigating whether the UK’s Apple notice violated the CLOUD Act, an agreement between both countries that bars the other from issuing demands for citizen data.

“If a company offered a backdoor without its customers knowing about it, it would be a massive violation of privacy and trust,” said Klosowski. “Even taken at face value, these sorts of backdoors put everyone at risk of hacking, identity theft, and fraud, because there is no way to ensure only the ‘good guys’ would have access. As we’ve seen in the past, bad actors will find a way into these backdoors.”

The full ramifications of Apple’s decision to withdraw ADP from the UK have yet to unfold. Britain isn’t the only nation that has a beef with end-to-end encryption — several EU countries and other “Five Eyes” alliance members have expressed interest in weakening the security method, arguing that it hampers efforts to crack down on child sexual abuse material and criminal activity.

This situation could be seen as a successful test of the UK’s overreaching surveillance powers that may inspire other governments to adopt the same approach. The US and Australia have already proposed laws with similar powers to the IPA’s technical capability notices, and the US, in particular, has tried and failed to crack open Apple’s user security before.

Unless a company impacted by these notices dares to violate legally binding gag orders, the IPA can either force targets to provide secretive snooping access or force them to remove the very barriers it installed to prevent it from happening in the first place. Either way, they have nothing to lose — we do.

https://www.theverge.com/policy/621848/uk-killing-encryption-e2e-apple-adp-privacy