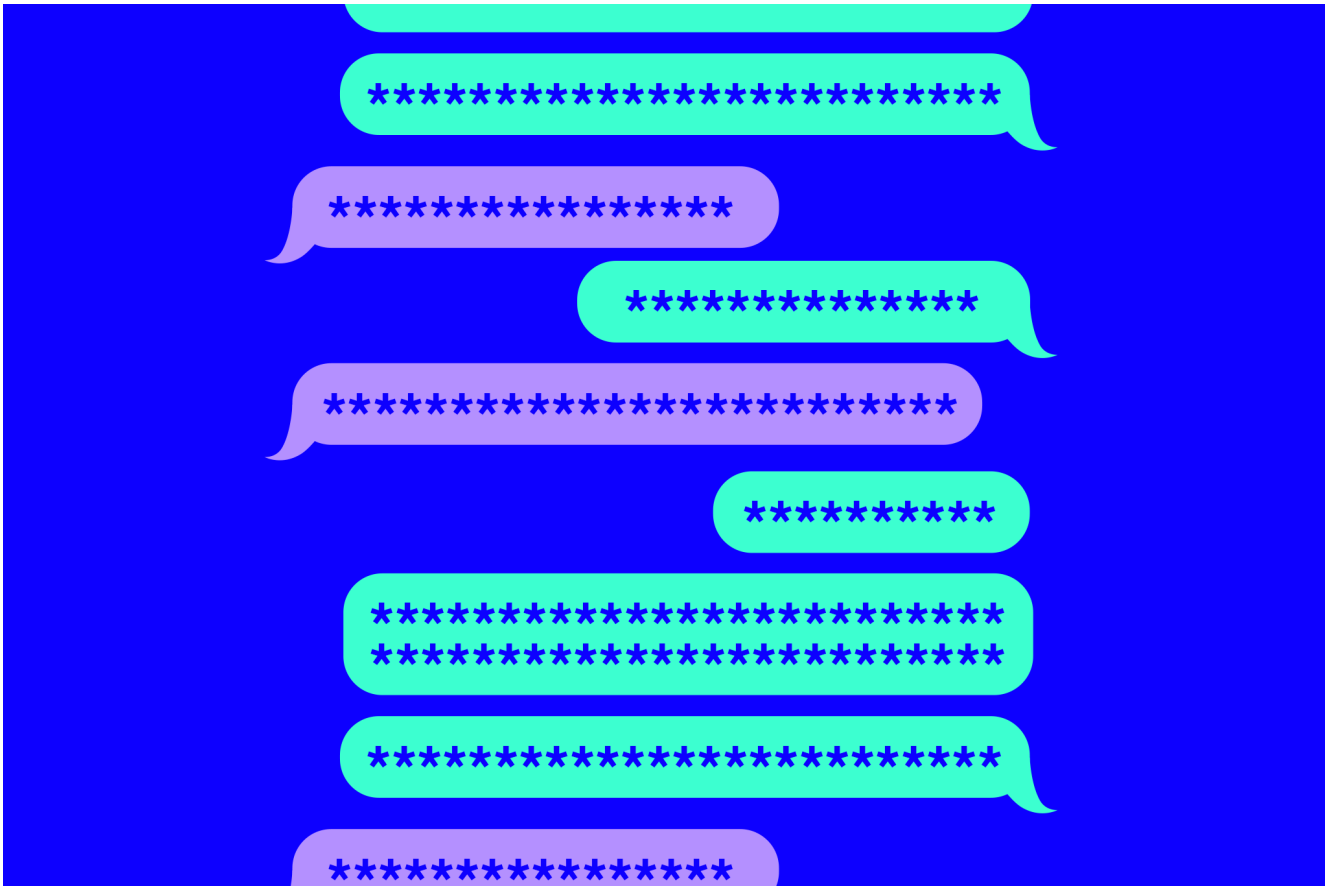
The UK’s war on encryption affects all of us



The encryption wars have reached a fever pitch, and the most contentious battle is not happening in the United States, where much of the action has been in the past — like the government’s efforts to restrict exports of encryption software until the 1990s and the FBI’s standoff with Apple in 2016. It’s in the United Kingdom, where the government has reportedly ordered Apple to give officials blanket access to iCloud users’ encrypted backups. And the order allegedly didn’t just apply to UK users — it demanded backdoor access for users *worldwide*.

The secret order, first reported by *The Washington Post*, was issued in January under the auspices of the UK’s Investigatory Powers Act of 2016. Apple’s compliance or refusal will have ramifications far beyond the UK, potentially making users less safe and signaling to other governments that they, too, can

seek backdoor access — a way of bypassing encryption — to users' information via legislation.

"Simply put, the message the UK government is sending is that its own citizens cannot expect its government to respect their privacy, and that it is willing to put their security at risk from all manner of bad actors like hackers and thieves because it cannot tolerate the ability to have a private conversation online," Andrew Crocker, surveillance litigation director at the Electronic Frontier Foundation, told *The Verge*.

Apple can appeal the ruling to a secret panel, but per the *Post*'s reporting, it can't delay complying with the order during an appeal. And the UK's Home Office would prohibit Apple from telling users that the government can now access their encrypted backups. This obviously creates a huge problem for Apple, which has built its reputation on safeguarding user privacy.

"Apple should be transparent with its users about how it's responding to this threat to their privacy and security," Greg Nojeim, the director of the Center for Democracy and Technology's Security and Surveillance Project, told *The Verge*. "It remains to be seen whether this move to weaken global cybersecurity around the world will hold, or whether the UK will back off."

Apple did not respond to *The Verge*'s request for comment.

For now, bystanders are left guessing. "If Apple does not appeal — if we don't see or hear about an appeal — does that mean they have complied?" Joe Jones, the director of research and insights at the International Association of Privacy Professionals, told *The Verge*. "If they complied, that creates a precedent not just for the UK, but for many other law enforcement authorities around the world."

It's Apple's policy to respond to law enforcement requests for data. Until 2022, iMessage might have been end-to-end

encrypted, but iCloud backups were not, so a warrant would typically result in the police getting access to your phone. But that year, Apple implemented end-to-end encryption for iCloud backups under a feature it called “Advanced Data Protection.” Though users have to opt in to Advanced Data Protection, this feature rendered Apple’s compliance with governments much less useful for law enforcement than before.

Security experts say, however, that the company’s resistance to backdooring has less to do with taking a stand against governments and more to do with baseline cybersecurity.

Governments are locked out of encrypted iCloud backups “because everybody is locked out of it, so that hackers can’t get in,” Ciaran Martin, the former head of cybersecurity at the UK’s Government Communications Headquarters — their equivalent to the NSA — said on a recent interview with the BBC. The issue with backdoors, Martin continued, is that there’s no way to build one that lets law enforcement in and keeps everyone else out. “If you build a door, other people will try to get in,” he said.

But according to Martin, the fact that the order is no longer secret could prevent it from being effective. “For the order to work, it has to not be known about by the criminals and the offenders,” he said.

Previous matchups between tech companies and governments over backdooring have had decidedly mixed results. In 2016, Apple and the FBI were involved in a bitter legal battle over the tech company’s refusal to unlock the iPhone of one of the San Bernardino shooters, which Tim Cook described as a fight to “help you protect your data and your privacy.” The feds needed the password because, a few days after the shooting, someone with access to the phone triggered a password reset of the shooter’s iCloud account, effectively locking law enforcement out.

Microsoft’s refusal to give federal law enforcement access to emails stored at a data center in Dublin, Ireland, almost led to a US Supreme Court case – which was dropped after Microsoft and other tech giants, including Apple, Amazon, and Google, threw their support behind the CLOUD Act.

Given Apple’s public comments, the company is unlikely to comply with the UK order. “There is no reason why the UK [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,” Apple told Parliament in March.

Rather than comply, people familiar with the matter told the *Post*, Apple may stop offering encrypted storage to UK-based users – but that still wouldn’t address the Home Office’s demand that Apple let its officials access the encrypted backups of users around the world.

“The challenge for that approach is that the UK’s Investigatory Powers Act is extraterritorial,” Jones said, which could lead to a “lengthy, protracted legal process. And these lengthy and protracted legal processes often spill out into diplomatic and political issues as well.”

https://www.theverge.com/policy/612136/uk-icloud-investigatory-powers-act-war-on-encryption