

# The UK demands the ability to access Apple users encrypted data.



The government of the U.K., by the Home Office under the Investigatory Powers Act (IPA), has made a demand to Apple to be given access to the encrypted data stored by Apple users worldwide through its cloud service. As it stands, only a person with an Apple account can access any data that is stored in this way, and not even the tech giant can gain access to it.

The right to privacy is a fundamental human right guaranteed **by Article 12 of the Universal Declaration of Human Rights**. Apple, on their website, in concurrence with this undeniable fact, brandishes the right of privacy as a “core value” of theirs and avows to uphold the privacy of its users, to which this “backdoor” being demanded by the government of the UK will go against.

The demand of the U.K. government covers all content that is stored using a system Apple refers to as “Advanced Data Protection (ADP)”—a system that makes use of end-to-end encryption, where only the account holder can access the data stored by them. An iPhone that is backed up with encrypted data consists of saved passwords, Wi-Fi credentials, and other volatile data that are needed in the event of a phone being lost, stolen, or damaged.

Although it is unknown the amount of people who opt to use this ADP, it is perceived that this demand of the U.K. government is to be implored in the event of a national security and to be used on an individual basis, taking into account the appropriate legal processes in accessing data. But cybersecurity experts have reached the agreement that, whereby assent is given to such demand, it will only be a matter of time before such access is gained by bad actors.

The Legal Director of Privacy International sees this demand as a precedent that will embolden abusive regimes all over the world. Apple may desist from offering the encrypted data services in the U.K. rather than breaking the trust and security promises it has made to its users everywhere. Be that as it may, there is no doubt that there is a larger possibility that acceding to this demand may lead to a floodgate effect with a bigger negative effect than the benefits hoped to be reaped.

Conclusively, if the UK government's demand for access to Apple users' encrypted data is to be met, it would be exceedingly needed for this new found power of the government to be checked so that it is not used arbitrarily.