fipr foundation for information policy research

FIPR explainer of the issues posed by the Home Office Technical Capability Notice to Apple

What has Apple been asked to do by the UK Home Office?

On 7th February 2025, the Washington Post reported that the UK Home Office had issued Apple a Technical Capability Notice (TCN) under the Investigatory Powers Act. The subject of this notice was Apple's Advanced Data Protection (ADP) service - with the Home Office issuing a blanket order to facilitate access to the service covering Apple's entire worldwide user base. Companies are barred from revealing whether they have been served these notices - even to legislative bodies like the US Congress. Following the leak, Apple publicly withdrew the ADP service for new users in the UK on February 24th 2025, refusing to implement what it describes as an unacceptable weakening of its encrypted protective services.

A Technical Capability Notice is an order given by the UK Government to a service provider. Most providers of secure encrypted services develop these to be 'secure by design'. Only the users have access to the keys that can unlock their data - so even the provider cannot access the content of people's communications or files. A TCN changes this - it requires the provider to retain the capability to remove the security protections on their product, in order to give UK law enforcement or security services access to the data of the service's users. This permits bulk access to the data on the service - so rather than compromising a single individual who is suspected of a crime, it grants access to the data of all users of the service. Apple - the service provider - is not allowed to reveal the technical details of how it permits this access, or the existence of the order itself.

Why are these orders controversial?

Although encryption is a highly technical field, the technical argument is actually the simplest even if it rests on complicated mathematics: a backdoor is a hole in a security system, and you cannot make a hole that only "good guys" can use. Requiring a backdoor in encryption is like requiring all households to deposit a front door key in the local police station. In today's world, in which cyber attacks and data leaks are rampant, the risks to privacy and personal security are obvious.

Backdoors generally take the form of either (1) a 'master key' held by a government body, (2) a deliberate mathematical weakness built into the encryption used in a system, or (3) a capability retained by the provider of the service to allow access in response to an order. The TCN uses the third kind - in which the provider changes the design of the service so that they can unlock access to data and communications when given this order. This changes the kind of security that these systems can provide for their users. A well-designed encrypted system can make scientifically testable guarantees about the level of security it provides, backed up by the mathematics of cryptography. But when a provider designs a deliberate weakness into the encryption that can be used to allow access, this creates a vulnerability that can be exploited by attackers, including organised crime groups and nation state hackers. Where providers include an 'off button' that allows them to decrypt the information themselves in response to a request, the weakest link in the system is now no longer the cryptography and the software - it is the staff working for the service provider, who can now be blackmailed and threatened, or sent a legal order by any government in the world.

The human rights issues are also clear: encryption is a tool by which individuals exercise their rights to freedom of expression and the right to private life, which includes the right to be protected against "arbitrary or unlawful interference". Providing the means for the state to choose at any time to inspect the contents of encrypted data clearly enables that "arbitrary interference" and is easily abused. The secrecy of the TCN regime means that these orders are not open to public scrutiny.

What alternatives do law enforcement have?

Law enforcement and policymakers often make the argument that encrypted services provide a ‘safe haven’ for criminals or make investigation of serious crime impossible. In fact, law enforcement have many alternatives for investigating crimes in which encrypted services are used. There is ample evidence that successful prosecutions are possible even where suspects have used end-to-end encrypted communications. Criminal activities leave a wide variety of traces that can be collected by law enforcement through traditional surveillance methods, communications and financial data access, informants, and open source intelligence gathering. The Investigatory Powers Act (2016) allows law enforcement to carry out targeted hacking of devices in order to expose their communications without ‘breaking’ the encryption. This is different from a TCN-style backdoor - which permits ‘bulk’ access to all of those who use the service - as it is targeted to individuals for whom there is a reasonable suspicion of involvement in serious harm. An example of this is Operation Venetic, in which law enforcement conducted targeted compromise of Encrochat encrypted devices.

What is the wider context?

Apple is an American company and there is growing bipartisan disquiet over the TCN in the USA. In particular, the fact that the TCN would also compromise the privacy and security of US users, and the requirement for Apple to refuse to confirm the existence of the order or answer questions about it - even when asked by, for example, a congressional committee - are of concern. It is possible that other US tech companies have been served, and complied with, these notices. Both President Trump and Vice-President Vance have criticised the TCN directly in the media. More generally, the application of the TCN to include all global users brings out potential legal conflicts internationally.

Those causing serious harm often do not need anonymity - instead, they rely on institutional and social power. The marginalised communities often invoked by proponents of backdoors are in fact disproportionately affected by the harms of bulk law enforcement surveillance. The needs of victims and survivors are extremely important, and we do not dismiss the serious harms caused by crime. However, we argue that the needs of justice would be better met by empowering and supporting victims and survivors, rather than undermining their autonomy, security, and privacy by granting law enforcement bulk surveillance powers over the general public.

Dr Ben Collier, Chair, Foundation for Information Policy Research
With contributions from Peter Sommer, Wendy Grossman, Guy Herbert, and the FIPR membership