

Apple - Written Evidence (June 2025)

The House of Commons Science, Innovation and Technology Committee one-off inquiry into phone theft

Apple submits these written comments as follow-up to the oral evidence provided by Gary Davis, Senior Director, Regulatory Legal (EMEIA) as part of the Committee's one-off inquiry to phone theft.

Introduction

Apple appreciates the opportunity to provide further information to contribute to the Committee's inquiry into this important issue.

Apple has recognised for many years the impact a theft of one's phone has on victims and has taken strong and continuous action over that period. We sympathise with people who have had this experience and we take all such incidents very seriously.

We are committed to safeguarding our users to the very best of our ability, and we have been working on this issue from a hardware, software, and customer support standpoint for the last 16 years. We have made and continue to make significant investments to create industry-leading tools and features to put control in the hands of our users in the event of theft, and importantly to discourage criminals from stealing phones in the first place. These include the "Find My" App and Remote Wipe feature first introduced in 2009, Lost Mode in 2012, Activation Lock in 2013, Stolen Device Protection and the extension of Activation Lock to spare parts in the last year alone (2024).

We also have a strong track record of collaboration with police forces and other law enforcement agencies across the globe and in the UK, particularly the Metropolitan Police, to tackle device theft. We see this as absolutely necessary as traditional policing will always remain important in this area. This includes our prompt response to specific law enforcement requests for data, supporting larger investigations and expanding our ongoing partnerships between law enforcement and teams within Apple, including our Retail Security and IP infringement teams. As we have made clear on a number of occasions we stand ready to increase this support as necessary to meet the needs of law enforcement as they pursue investigation and enforcement activity.

In this submission we cover the work Apple has done in this area to date, including very recent innovations, and also address some of the Committee's questions from the oral evidence session in more detail.

It should be clear to the Committee that there is no silver bullet in this space. Industry, Government and the police have a responsibility to work closely together to remove to the maximum extent possible the incentive for criminals to target mobile phones for theft. This requires a combination of technical solutions which will need to be kept under constant review as criminals evolve their methods, and close co-operation to assist law enforcement target the criminals engaged in this behaviour so that they can face the full consequences of this criminal activity.

Apple's device security features

We work tirelessly every day to protect our users' accounts and data, including building and introducing additional protections to strongly discourage criminals from stealing devices in the first place and then in the event a user's device is stolen. Key features include:

Find My & Lost Mode

Introduced in 2009, Find My allows a user to locate a lost device, and to share this information to aid the police when looking into a theft. Since 2012, a user can also enable Lost Mode through the Find My app, which remotely locks the device and removes the ability to make payments with any credit, debit and prepaid cards that are linked to Apple Pay on the device.

In the UK, over 90% of users have Find My enabled. In iOS17 we made changes to the set up flow for new devices to more strongly encourage users to enable Find My and make clear the potential security consequences of not doing so.

Activation Lock

Launched in 2013 explicitly to discourage criminals from stealing devices in the first place and assist our users when dealing with lost or stolen devices, Activation Lock runs in the background to make it more difficult for someone to use or sell an iPhone or iPad if it's ever lost or stolen, as it locks the device to the user's Apple Account. Apple also provides guidance to individuals shopping for potentially used iPhones to check for Activation Lock before purchasing.

Apple also does not accept devices for repair or replacement, or for trade-in purposes, if Activation Lock is enabled on the device.

Activation Lock is turned on automatically when a user has enabled Find My.

Stolen Device Protection

Introduced in 2024, Stolen Device Protection prevents someone who has stolen the device and knows the passcode from making critical changes to a user's account or device.

Some actions such as accessing stored passwords and credit cards require a single biometric authentication with Face ID or Touch ID — with no passcode alternative or fallback — so that only the user can access these features.

Critical changes such as changing the Apple Account password will require the user to wait an hour and then perform a second Face ID or Touch ID authentication in a place where the device is normally.

In the event that an iPhone is stolen, the security delay is designed to prevent a thief from performing critical operations so that the user can mark their device as lost and make sure their Apple account is secure.

Stolen Device Protection has to be enabled by the user so that a user knows how to manage the device if it is away from a familiar location.

The UK has one of the highest rates of adoption of Stolen Device Protection, with over 55% of eligible devices protected - this is high for a new feature, and higher than the worldwide adoption rate. Since introducing Stolen Device Protection, when users have upgraded to a version of the operating system with this new feature, it is presented to them and they are encouraged to turn it on.

Remote Wipe

First introduced in 2009, this feature gives the user the ability to remotely erase all content and settings from their device in the event their phone is lost or stolen.

Face ID or Touch ID biometric authentication

Face ID and Touch ID make it easier for users to have strong passcodes (6 digit by default) by not requiring passcode entry during most unlock operations. In addition, use of biometrics in public means that thieves don't have the opportunity to surveil users and learn their passcodes by observation.

Two Factor Authentication (2FA) iCloud roll-out

The committee will be aware as we are of the issue of phishing for account details once a phone has been stolen, or aggressive messages asking the user to remove their Apple Account details from the device so the thief can make use of it. This is one of the reasons why our phishing protections are so important, and it is notable that we have the largest 2FA rollout we're aware of in the world, with over 95% of iCloud accounts protected by two factor authentication.

Recovery Key

A recovery key is an optional security feature that helps improve the security of a user's Apple Account. If a user loses access to their account, they can use their recovery key to reset the password and regain access.

Activation Lock for spare parts

As we informed the Committee, the market for stolen devices is complex. Activation Lock is aimed at criminals seeking to reactivate stolen devices. It is clear however that there is a market for parts from stolen devices to be used for phone repairs. This is an area that also requires significant ongoing attention to discourage criminals from targeting phones for this purpose. Apple believes this market may be significant and we wish to take strong action to render such parts unattractive for repair purposes.

Apple has invested substantial resources in safeguarding our devices' components from unauthorised use and therefore to disrupt the markets for stolen parts. In April 2024 we announced that, from October 2024, Activation Lock would extend to spare parts. This was intended to help combat the monetisation of secondhand parts, and thus, reduce the incentive to steal an iPhone.

If a device undergoing repair detects that a supported part was obtained from another device with Activation Lock, customers will be informed during the process. This is expected to prompt customers to seek explanations from the part's seller or contact the authorities.

For individual parts that require pairing for authentication and optimal performance, they will function if installed in another iPhone of the same model but cannot be paired for optimal performance. This means certain features are negatively impacted.

Locked / hidden apps

Introduced in September 2024, this feature allows users to lock or hide certain apps which can only be opened with biometrics, which provides an extra layer of security in the event of theft e.g. locking away banking apps. This feature is compatible with Stolen Device Protection - so locked and hidden apps do not support passcode as a fallback when Stolen Device Protection is active.

We believe the introduction of these industry-leading features spanning the last 16 years, with new features introduced as recently as last year, demonstrate a strong track record of investing and innovating to protect our users' devices and data as best as we possibly can, and that we do not stand still in this effort. We are constantly working to combat theft and fraud and are committed to iterating and developing new features that we believe will make a positive difference.

Additional support for customers

We use a variety of ways to provide comprehensive and dedicated support to our customers in the event their phone is stolen, and to share information about relevant security features.

- **40 Apple Retail Stores across the UK** (including 8 around London). Store teams are trained on device security and share advice with thousands of customers each day concerning the protection of their devices and safeguarding of their private data. We are also there to support those visitors who have just had devices stolen and we assist by blocking devices using the Find My app (if available) and suggesting next steps, whether that involves reporting to law enforcement or making insurance claims.
- **Today at Apple** - We run free training classes for our customers which are available at all our UK stores, known as "Today at Apple". One of these classes, available on request in each store, is called "Taking charge of your privacy on iPhone". Customers explore built-in privacy and security features that put them in control of their data and information. They learn about passwords, Mail Privacy Protection, Location Services, and more, so that, should the worst happen and their device is stolen, they know how to protect their data and block the device immediately.
- **Apple Online Store Contact Centre for UK customers** - Our team of dedicated call agents at our UK facing Online Store contact centre offer the same support remotely Monday–Friday 08:00–20:00 and Saturday–Sunday 09:00–18:00.
- **Support Articles** on apple.com also provide our customers with detailed security information to help protect their devices. Examples include:
 - Security and your Apple Account: <https://support.apple.com/en-gb/102614>
 - Stolen Device Protection: <https://support.apple.com/en-gb/120340>
 - Activation Lock: <https://support.apple.com/en-gb/108794>
 - Lost Mode: <https://support.apple.com/en-gb/guide/iphone/iph7cc193cfc/ios>

- **Marketing** - we just released a new cross-channel marketing campaign to build greater awareness of the Stolen Device Protection feature. We are planning to re-run this marketing campaign from July to October.

Working with law enforcement

We have worked closely with law enforcement on the issue of phone theft for many years. We see this as absolutely necessary, as traditional policing will always remain important in this area as criminal behaviour keeps evolving. We have engaged intensively with the Home Office and Metropolitan Police in particular over the past year, working collaboratively to tackle high rates of theft in London.

A core part of this work is our day-to-day support for police on active investigations. We respond to standard law enforcement requests for data regarding stolen devices, on average, within 48 hours. We continue to believe there is an opportunity to further support UK law enforcement in relation to active investigations of stolen devices.

We stand ready to increase our support as required and as requested by law enforcement bodies as they undertake enhanced enforcement and investigation activities.

We also have expanding partnerships outside of our law enforcement requests teams. Our Global Security, Retail Security and IP enforcement teams work tirelessly with local Police forces to target criminal activity. Recent activity includes:

- **IP / counterfeit teams** - Apple has dedicated teams working with law enforcement to detect and disrupt the counterfeit parts market. In the UK this includes working closely with the City of London Police, which has particular expertise in both economic crime and intellectual property crime, as well as teams within the Metropolitan Police as part of their recent initiative Operation Reckoning. This has seen our teams supporting police raids to identify stolen and counterfeit products which has led to arrests - we are actively liaising with the police to support this enforcement activity on a continuous basis.
- **Retail Security** - Our retail security team has supported the Metropolitan Police with recent intensification activities to tackle organised store thefts that targeted demo iPhones at Apple Retail Stores. The partnership has proved to be constructive. Both teams are proactively seeking opportunities to further collaborate to build on this work; this has included hosting a recent meeting with the Met in Battersea.
- **Equipping the police to share useful information with users** - We have worked to provide the Metropolitan Police and other police forces with easily accessible guidance for our users on how to best protect their device, and what to do if their device is stolen. This guidance has been produced for police forces to easily share with victims of theft who have reported their phones stolen; and for Mobile UK to share with the mobile network operators for the same reason.

Stolen parts market

We acknowledge that the market for stolen phone parts contributes to mobile phone theft. Stolen phones can be disassembled into their components and resold in the UK and internationally. In our experience, the combined value of a phone's parts can sometimes

even exceed the original device's worth. Regardless, the device itself is a valuable item, and if a stolen device is useless to a thief because it cannot be reopened or reactivated due to the security protections, then it will most likely be stripped for parts.

While all parts have value in the stolen, secondhand, or counterfeit market, the most valuable parts are those that are challenging to counterfeit, particularly electronics. There is a premium on genuine parts, which are those taken from stolen phones, rather than counterfeit ones.

This is why Apple has invested substantial resources in safeguarding our devices' components from unauthorised use and to disrupt the markets for stolen parts, including the recent extension of Activation Lock to repair parts.

Resources and accountability

The Committee asked us to provide details of the level of resource and investment we commit to device security protections. Because of the way Apple is structured, spending or staff are not recorded or allocated by product or feature. Many different teams and functions contribute to any new feature. While we cannot provide a specific figure for any one feature we've released, it would be fair to describe these as multi million dollar investments. By way of reference, Apple's global R&D spend in the financial year ending September 2024 was \$31.37 billion.

The safety and security of our users and their devices are of the utmost importance to Apple. As such, the executive team of the company - the most senior people in our business - are responsible for and are fully involved in decisions taken in this area. This is why Apple has released solution after solution in this area in order to make it unattractive for criminals to steal iPhones. We are committed to continuously innovating in this space in order to ensure that criminals have no financial incentive to steal our devices.

IMEI blocking

We fully recognise the Committee's interest in further technological actions that could be taken to tackle phone theft, and that one such area of interest is whether device manufacturers could block the re-activation to their servers of devices with an IMEI that has been reported stolen. We have previously expressed our view, as we did in our oral evidence to the Committee, that we have concerns with this approach if wider privacy and security implications are not sufficiently considered. We outlined those considerations at the Committee.

However, as we stated in our oral evidence to the Committee, Apple is now considering how IMEI-blocking could be enacted, giving appropriate consideration to the potential risks and trade-offs.

ENDS