



Dame Chi Onwurah MP
Chair, Science, Innovation and Technology Select Committee
House of Commons
London
SQ1A 0AA

8 August 2025

Dear Chair

Thank you again for inviting Google to provide oral evidence to the Science, Innovation and Technology Committee. We treat phone theft extremely seriously and are grateful to have had the opportunity to engage with the Committee.

Google is absolutely committed to addressing the challenge of device theft. This requires extensive cross-functional collaboration across Google globally, with expertise from multiple teams working together to proactively secure users' Android devices and data before, during, and after a device theft attempt. This includes core product and engineering teams such as the Android Platform Security & Privacy team and the Android Find Hub team building advanced security features into Android devices. Depending on the particular feature, other Android teams may also contribute.

We also partner with the original equipment manufacturer (OEM) community to help protect devices more widely. The Android Partner Engineering team engages with Android OEM partners to incorporate OEM feedback and ensure any integrations with their devices work effectively. There are also teams managing the infrastructure that all these products are built in, teams managing the release processes, quality assurance teams, marketing teams to make users aware of the features and UX researchers, and designers building solutions that are user-friendly and usable.

Building and deploying advanced security features requires distributed responsibilities across Android and Google more broadly. That's because these features touch on everything from access to the device and the various settings and functions, as well as remote access to services. Given the complexity and cross-functional character of this effort, it is not possible to give a precise figure of the number of employees or where they are based. Additionally, there is a broader ecosystem aspect covering a range of tasks, such as communicating the features to network operators, retailers, financial institutions, NGOs, government agencies and directly to users.

Our solutions are focused on what we can build in the operating system to safeguard users from theft. Our top priority is the safety of our users, which involves both protecting their data and reducing the incentive for theft. We have therefore implemented a comprehensive suite of industry-leading features, from hardware to software, in order to create a robust security posture.

For example, Find Hub is where Android users can find, lock, erase or play a sound on any lost Android device. [Factory Reset Protection](#), a feature for many years, prevents resetting the device and re-using it (or re-selling it to another user) by requiring the (previous) owner to take an action before the device can be set up by a new user. If they do not do this, the device is unusable as it cannot complete setup, and cannot be used as a working device.



These features are on by default and we are continually innovating to address the challenges of phone theft. Our most recent software releases, Android 15 and Android 16, further strengthen the protection offered by Factory Reset Protection by restricting all functionalities on devices that are reset without the owner's authorisation.

We continually keep our approach under review. Other techniques, such as blocking devices via an IMEI number may be a practical option from an operator perspective. As the operating system (OS) provider, we believe we can better serve users by giving them direct control over blocking their phone via their Google account. Using tools like those described above, users can effectively block their device, regardless of whether they have also reported the device as stolen to law enforcement, their mobile phone network or other authorities, and regardless of which jurisdiction the device was stolen in or moved to. Our protections, therefore offer a robust solution that is fully aligned with privacy, security, consumer and other regulatory aspects, and maintains our commitment to place users first.

We do not have information on phone theft for parts but there is a consensus that this is a motivation for phone thefts. There have been a number of press reports on this issue (see, for example, the [FT](#), May 2025¹ and the [Daily Mail](#), March 2025²).

We are committed to working with law enforcement and industry partners, including the GSMA, and remain open to further exploring further options to disincentivise phone theft. We believe this requires a collective effort and we support collaborative efforts to collectively improve device security with the government and the wider industry.

Please let us know if you have any further questions.

Yours sincerely,

Simon Wingrove
Software Engineering Manager, Google

¹ Inside China's 'stolen iPhone building', William Langley, 21 May 2025, Financial Times

² Mobile phone thefts have TRIPLED in four years as criminal gangs riding e-bikes fuel booming underworld export trade to China and Nigeria, Elizabeth Haigh, 11 March 2025, Daily Mail