HOUSE OF COMMONS

Science, Innovation and Technology Committee

Oral evidence: Phone theft, HC 882

Tuesday 3 June 2025

Ordered by the House of Commons to be published on 3 June 2025.

Watch the meeting

Members present: Chi Onwurah (Chair); Emily Darlington; Dr Allison Gardner; Kit Malthouse; Steve Race; Dr Lauren Sullivan; Adam Thompson; Martin Wrigley.

Questions 1 – 123

Witnesses

I: Darren Scates, Chief Digital Data and Technology Officer, Metropolitan Police; and Commander James Conway, Commander/phone theft lead, Metropolitan Police.

II: Dion Price, Chief Executive, Trustonic; and Katarina Zotovic, Senior Analyst, S-RM.

III: Gary Davis, Global Senior Director, Privacy & Law Enforcement Requests, Apple; Simon Wingrove, Software engineering manager, Google; and Nabil Ahmed, Head of Technology & Digital Services, Samsung Electronics Ltd.

Written evidence from witnesses:

- Metropolitan Police
- Katerina Zotovoic
- Trustonic

Examination of witnesses

Witnesses: Darren Scates and Commander Conway.

Chair: Welcome to today's one-off session of the Science, Innovation and Technology Committee on phone theft. Phone theft is a huge issue in this country, which appears to be, from the figures I have seen, the phone theft capital of Europe. It is an issue across the country, but over 70% of those phone thefts take place in London. It is also an issue in which various members of the Select Committee have significant professional expertise, which is why I am going to ask Kit Malthouse, as a former policing Minister and deputy Mayor for London for policing, to kick us off by welcoming the first panel and starting the questioning.

Q1 **Kit Malthouse:** Thank you very much indeed. Welcome to you both and thank you for coming. I walked out of my house this morning to take my kids to school. I got into my electric car and, as we were leaving our London home, two young lads on bikes with black masks came past us. I thought, "Ah, this looks quite interesting." A woman was standing on the corner of the street who had obviously been jogging. She was looking at her phone and they attempted to rob her. I beeped my horn. As I beeped it, she turned around and, as a result, they both fumbled the phone, and it fell to the ground. They legged it; she picked up her phone and jogged on.

This is a common experience and something that people witness every day in London. Can you start by giving us a sense of the scale of the problem in London, and also what it feels like in the rest of the country, if you have information? In particular, do you have hard numbers around frequency, value, numbers—that kind of thing—so we can get a sense of the problem?

Darren Scates: Thank you, Committee, and thank you, Kit, for the question. This is an organised criminal enterprise that we are dealing with. It is an international enterprise, although, as the Chair described, it is particularly acute in London. We see similar numbers in Madrid, Paris and Barcelona, and certainly on a per capita basis they suffer very similarly to London. In London in 2024, unfortunately, about 80,000 smartphones were reported as stolen. That compares to 2023, when the number was 64,000. We have a growing and very serious problem that we are dealing with.

Stolen devices change hands on the streets for between £300 and £400. You probably pay around £1,000 to maybe £1,300 for a phone, and they still have a street value of about £300 to £400. That is when criminal gangs acquire them from the kinds of individuals that you described. We know that about 80% of devices that are reported stolen to us are Apple devices. That is because they are probably being targeted for their value and/or there is a greater incentive to report an Apple device as stolen because they tend to be a higher value item.

We have done some research into what happens to the devices, as you would expect. What we find is that about 75% of them, we believe, are actually moved abroad. The prime locations at the moment—I am sure this will vary—will be Algeria and China/Hong Kong. About 28% go to each of those two locations. That is the scale of the international problem and the London problem. If I might, I will ask Mr Conway to describe a little bit about the issue that that then creates for Londoners and for the police in how we respond.

Q2 **Kit Malthouse:** Before you do that, I have just a couple of follow-up questions. How do you know where they are ending up? You said it has gone up from 64,000 to 80,000 last year. What are the numbers looking like this year? Is it up or down? Is that exponential path still increasing?

Darren Scates: I will capture the "How do you know?" and will then ask Mr Conway to talk about this year's numbers, if I may. In terms of how we know, around a year ago we provided a sample of device serial numbers to the cloud providers—Google and Apple—and asked them to tell us what countries, if any, they reconnected in.

Q3 **Chair:** The serial number, not the IMEI?

Darren Scates: Sorry, it is the IMEI number specifically, yes. It is the serial number of the modem in the device, which is the IMEI number. We provided that to Google and Apple around a year ago. We provided a sample of around 4,000 devices. The statistics I have just described are the statistics that were then provided to us by Google and Apple for where those devices had effectively popped up on the internet in different parts of the world. That was the source of our numbers as to where we believe they are going.

Q4 **Kit Malthouse:** It is not that you have identified how they are getting there, but you know that they are getting there.

Darren Scates: We have had a number of successful operations—for example, seizures at airports and ports where we have, on occasion, been able to track phones, although there are some challenges with that which we can cover a bit later. We make a seizure at a port, and we can see where a parcel, for example, was destined. The primary source of information was the digital information that was provided for us.

Q5 **Kit Malthouse:** Commander?

Commander Conway: I will touch on the harms and then come back to that point about the impact in recent months. The scale of theft of phones had a street value of around £20 million last year. The replacement value of those phones—members of the public and insurance companies having to pay out to replace them—we estimate at around £50 million last year. As we have talked about, around half of the robberies in London are mobile phone-related or phones that are stolen. It is driving our robbery problem. Around two thirds of our thefts in

London relate to mobile phones. This is also driving our theft problems and the increases that we have seen in recent years, as Kit noted.

If you take a step deeper, 65% to 70% of our knife crime is produced by our robbery problem. It also drives a significant chunk of our violence challenge in the capital and across the UK. In that space lies the exploitation of young children, young people, into gangs. As Darren says, this is largely an international organised crime phenomenon driven by the criminal economics that the speaker on your innovation showcase panel was alluding to, and the difficulty in getting hold of smartphones legitimately in some parts of the world. It drives an international criminal economy where the source country for that commodity in that criminal economy is the UK and Europe, as we have just heard.

This has been a sharp focus for the Met and other large metropolitan forces for a couple of years. In recent months, we have seen a decline; in the first couple of months of this financial year, there was around a 15% reduction in thefts and around a 13% reduction in robbery, when compared to the opening months of the previous financial year. That is a sustained effort from the Met police from an enforcement perspective.

What is very clear, given the scale and the challenge that Darren outlined, is that the enforcement aspect alone will not be sufficient to tackle the issue. We largely see it as a challenge across various strata. We have acquisition of phones in the UK through theft, robbery and other linked offences. We have a middle market element, which involves the collation of those phones by criminal gangs and the preparation for export. We have an export layer to China, Algeria and other parts of the world, as we described.

At the heart of that we have something which is perfectly legitimate when purchased lawfully—a mobile phone—but which becomes a criminal commodity when stolen, in much the same way that drugs, firearms or indeed human beings can become a criminal commodity, and are then susceptible to exploitation by international organised criminals. The difference is that the source of that commodity is the UK, not the end marketplace. Nevertheless, the harm generation created by that acquisition is considerable here in the UK.

Q6 **Kit Malthouse:** I have a couple of motivation questions. Why is London so particularly marked in being a target? Where is the value in the phone? I am assuming that it is the entire phone, but is it also parts?

Commander Conway: Both, we believe. Why London? Like any other marketplace, it is the economics that drive it, I would suggest. Again, we see it across other major cities in Europe. You already have organised crime networks well established in London. You have export and trafficking routes in and out of the UK that have a significant and long-standing serious and organised crime focus on London. Of course, you have a large population and a concentrated urban environment, where theft and robbery are easy crimes to commit.

In my previous role, I led for policing in Hackney and Tower Hamlets. We would regularly see criminal gangs who might, a few years ago, have been involved almost exclusively in drug dealing. They pivoted a few years ago back into mobile phone theft and robbery in a way we probably haven't seen since the early noughties. They exploit young people to become involved in that. The classic image is very much as you described earlier, Kit: teenagers on stolen bikes riding down the A10 corridor and committing 10 or 20 robberies or thefts on the go, packaging the phones very swiftly into silver foil or Faraday bags to make it more difficult for us to identify their ultimate location, and then swiftly passing them on to a middle market handler and, ultimately, transport out of the UK to the countries that Darren described.

Q7 **Kit Malthouse:** A final couple of questions from me. There is money to be made, obviously. My guess is that, even if you get caught, the sentence is a lot less than for drug dealing. There is a lot less jeopardy with this from the criminal justice point of view. I assume that is correct.

Commander Conway: Yes.

Q8 **Kit Malthouse:** What you are telling us is that there is a robbery every five or six minutes—or has been—and you think you are down about 15%. Some of that is through sustained police action. I imagine that some of that is because people in London now know that you don't get your phone out when you come out of the tube. No school kid gets their phone out as they leave the tube, as it is a target area.

Commander Conway: Yes.

Q9 **Kit Malthouse:** We were talking earlier about the car radio decline. There is a science and technology solution there, which is why you are in front of the Committee.

Commander Conway: Yes. To expand a little bit further, our understanding is that around 75% of the phones that are exported from the sample set that we have been able to analyse are then reconnected and utilised overseas. To your point about whether they are stripped down or simply resold and reutilised, if we extrapolate that, we assume that around three quarters are—

Q10 **Kit Malthouse:** Just one small technical question, as you raise that. If my phone is stolen from me and ends up wherever overseas, at all times it remains my property.

Commander Conway: Yes.

Q11 **Kit Malthouse:** If I tell my mobile phone provider to do something with that phone, that is perfectly legit because it is my property.

Commander Conway: Yes.

Q12 **Steve Race:** Thanks for those answers. You talk about phones changing hands. It is probably slightly more integrated than that. You also alluded

to child exploitation and the organised element. Are these phones stolen to order, even if it is, "I want 20 iPhones today"? Are they specifically asking young people to go and get them? What is your view?

Commander Conway: A mixture. Probably two broad themes emerge. One is criminal gangs who are themselves instigating and managing the theft. Certainly, in central London we see, either in shopping areas or in the night-time economy, gangs out stealing to order in that sort of sense. There is another layer, which is a demand-driven requirement: probably criminal gangs making it very clear that they would like certain types of phone. Unconnected to them, there are street gangs and more disorganised criminals going out and stealing phones and then passing them on to a handler. It is a mixture, but the demand signal is very clearly that they would like certain types of phone, and that is why we see particularly Apple devices featuring so prominently in the stolen devices.

Q13 **Steve Race:** We talked about how the crime at street level is connected in terms of the robberies, thefts and knife crime. What about at the organised end of it? Where is the money going? What happens to the money when it changes hands, and the phones are sold?

Commander Conway: It is difficult to determine at the moment. It is a large focus of a lot of our investigation at this stage. Much as I described the various strata, so the investigative response again mimics those three different strata. We are tackling the robbery element on the streets. We are focusing on the middle market element and trying to disrupt that handling activity. For example, in November 2024 four Algerian-linked individuals were convicted of an organised crime network involved in smuggling large quantities of phones out of the UK. Interestingly, they were involved in fraudulent access to the original phone holders' bank and crypto details, which we estimate probably resulted in around £5.1 million-worth of theft from those individuals.

It is not just following the cash and the phone and the transaction itself; there is also the secondary effect of fraud and other ancillary theft offences once the phone is removed. That is happening outside the UK, which, as you will appreciate, makes it a challenge for us to track.

Q14 **Steve Race:** How many people in London do you think are handling the phones to export them?

Commander Conway: I don't think we can estimate volumes at this stage.

Q15 **Steve Race:** Are there a number of gangs?

Commander Conway: We know where some of the hotspot areas are in London. Elements like the Find My phone technology, both in Android and Apple, are vital for us as an intelligence tool. It has its value on the individual phone you are trying to track. That phone has an even greater value and a sense for us when we aggregate the data and understand

where phones are potentially hubbing in London, but what that has not been able to give us at this stage is an estimation of the numbers of people involved. It is just the locations and the type of routes that we are starting to uncover that lead from the theft on the street to the activity in north Africa or China.

Q16 **Steve Race:** I suppose this is where I get confused. This is a big problem. It is a big social problem in London as well. It gives London a bad name. People view it as one of the big driving factors of London not being a very good place to be, to live or to go out. We know it is connected to knife crime. We know it is connected to organised crime, yet we don't seem to have got a grip on it from a crime perspective. It has been going up pretty exponentially until potentially this year. How is it prioritised within the police? What sort of funding and money allocation do you put towards it?

Commander Conway: Certainly last year, and into this year, theft, robbery and associated offences, the violence and knife crime that accompany them, are one of the primary priorities of the Met police. Across both local policing—your BCU, proactive detecting capabilities—and neighbourhood policing teams, we have been focused explicitly on this area. In fact, we would say that, to a large degree, that results in the tentative reduction that we started to see at the beginning of this year.

In terms of robbery reductions, probably since January 2024, we have seen it hit the top of a curve and there has been a downward trajectory since then. In the serious and organised crime space, we have more of our specialist investigative capabilities, up to and including things like the flying squad, involved in taking out that middle market area. That is the bit where we are less certain on the facts, figures and full extent of offending, just because, for many years, it has been a more hidden, covert aspect of the criminality, whereas the very visible and more obvious sign is the theft and the robberies on the streets.

Q17 **Steve Race:** I had my phone stolen, and I could track it to a specific place in south London. I blocked it and wiped it, but obviously the GPS acts slightly differently and separately from the phone. I let the police know that it was in a specific place in south London. I could then track it to a specific place in Algeria within two days.

You have that information. I did not get much back from the police, I have to say. I got a crime number and was told to pop off and sort it out myself. It did not feel like it was particularly valued as a crime. You have the information, and you have had it for quite a few years, but we do not seem to be getting to the point of having much intelligence about who is doing it. What are you doing with Border Force, apart from anything else? We know that the phones are flown out to Algeria. There are plenty of stories of people saying, "If someone is flying into Algeria, no questions asked if you've got five phones on you." You might get a quizzical eyebrow if you have 10, and more than 20 you might get pulled aside. What are we doing with partner countries? What are we doing with our

own border control to make sure that we can tackle it at that point?

Commander Conway: We are practically targeting handlers in the middle bracket you described, where the phone goes to a certain location. As I say, that is the value of intelligence aggregation, all the Find My phone data, which allows us to identify locations where we see a number of different phones being taken to. We can mount what often begins as a covert, but certainly a proactive, operation to target the handling group undertaking that activity. We work closely with the Home Office and DFT on the export control element. Not all of the export controls necessarily work in our favour in that space at the moment, but we are working more closely across Government to explore how we can further target and harden the borders. That has largely been about protecting against incoming criminal commodity. We are now looking to utilise and help protect against the export of criminal commodity, which is one of the challenges.

We have had some initial successes. At Heathrow, some months ago, we recovered 1,000 phones in a proactive operation, targeting the export element. With each of those operations we learn more about the criminal methodology of the gangs. As I say, we are working with DFT and the Home Office to determine how we can block off some of the routes out of the country. Some involve large-scale packaging and export as freight, in that sort of sense. Some of it, as you described, is couriers taking handfuls of phones out, often wrapped in Faraday bags, tin foil and so forth to try to conceal the passage of those devices.

It is about tackling the street end acquisition of the phone and tackling the middle market and organised criminal networks who are managing this crime phenomenon. We are increasingly focused on the export challenge, but, fundamentally, even that effort will only deliver a certain degree of impact against this crime area. Where we feel we can gain significant and additional impact is by removing the value of that criminal commodity. If the phone, when it moves abroad, cannot function as a smartphone, the economic model sitting behind it essentially evaporates at that moment. That is why our work with industry has been so crucial.

Chair: We need to move on.

Q18 **Emily Darlington:** I want to explore more around the export market. You have a problem in major European big cities feeding markets abroad. What kind of co-operation do we have with our counterparts in Paris or Rome, where this is happening?

Secondly, you say that the kids who are stealing them do not know who the couriers are going to be or how to deal with the export markets. What are we doing to tackle the people who are clearly getting the phones out of the country? It is not the kids on the bikes getting them out of the country.

Kit Malthouse: It is the middle market.

Emily Darlington: How are we actually tackling that? I will come back on the data point later. That is where you are getting scale. It is impossible for the police to be everywhere, including Kit's corner when he is driving the kids to school and—

Kit Malthouse: At 8 o'clock in the morning.

Emily Darlington: We get that, but where they are being aggregated and taken out of the country, people must be using similar tactics in other European cities.

Chair: Just come back briefly on that, and then we will move on.

Darren Scates: We are in contact with other cities. The mayor is in contact with other city mayors in Europe to look for their support. We are working closely with our serious and organised crime teams internally, as well as with the National Crime Agency. When we get a lead as to where the phones are going, we look to follow up on that, including to Algeria. We are in contact with the Algerian authorities. They have actually been very co-operative in helping us to track what is happening in Algeria, so we can get to the actual source of the problem. I think that is what is behind your question. How are we getting upstream?

What we also need help on, and I would like to cover it, is how industry—

Chair: We have less than 10 minutes left, so we will move on to some of those more technical questions.

Q19 **Martin Wrigley:** These things are very different from all the other things you have talked about with smuggling, because they are connected. The people who connect them are the networks. You have not actually mentioned the networks once in your entire discussion all the way through.

I wrote a "lost and stolen" system for Orange 30 years ago. It knew every IMEI of every phone on the network and we blocked them. There was an international blacklist. What the hell has gone wrong?

Darren Scates: There is an organisation called the GSMA, which links up the mobile companies within the UK and covers about 10% of network operators across the world. Notably, they have quite poor coverage in north Africa, or most of the continent of Africa, most of the far east and indeed the middle east. They actually have very poor coverage because the individual network providers in those countries have not signed up to the GSMA. While the GSMA give relatively good blocking in the UK for at least one IMEI number on the phone—a number of phones these days have several serial numbers and several modems effectively—that is probably why we see the majority of phones now going abroad. UK blocking is not perfect but it is not too bad.

We think network blocking is probably limited these days because of the preponderance of networks across the world, and GSMA only covering

10%. What we are in conversation with the cloud providers about—Apple and Google—is what they can do about stopping a smartphone being smart. The only thing that makes a smartphone smart is that it can connect to cloud services. Our ask—it is being considered by Apple and Google—is that at cloud level, which is an international level, they actually stop a smartphone's serial number connecting to their services if it is reported lost or stolen.

The GSMA, if I may say, was a brilliant start. It has helped significantly in the UK and in some international jurisdictions, but to give an international perspective, we now see the criminals moving their focus to countries with less good GSMA coverage, which is where we think the cloud providers may be able to help us.

Q20 **Chair:** To clarify that, you are saying that if one of the cloud providers is told a specific IMEI—a serial number, as you put it—has been blocked, you are asking them to prevent that phone from accessing cloud services.

Darren Scates: That is our ask—the Find My example that we heard earlier. It doesn't even need to involve the police, although we are obviously very happy to help and we provide all the IMEI numbers that we receive to the network providers in the UK. This is where an individual reports their phone as stolen. If I may say so, the cloud companies do a pretty good job of protecting their data. They lock the device, but it is very much then reliant on the device-level security to keep it locked. We would like them to actually block it at the cloud level.

Q21 **Dr Gardner:** I don't have many questions. I want to comment very quickly to Commander Conway. Thank you for raising the societal issues and that you link this with the exploitation of children and knife crime. You briefly mentioned that it is in other metropolitan areas. You compared London with the international market. Is it something that we will see rolling out across the country? Where London starts the trend, it sometimes filters out to areas such as Stoke-on-Trent. Is this something that I am likely to see landing on our doorstep?

Commander Conway: Robbery and theft are nationwide. I think there is a particular clustering in London. To a degree, we see a slightly lower level of clustering in other large metropolitan areas of the UK, such as Birmingham—

Q22 **Dr Gardner:** But you are collaborating with them.

Commander Conway: Very much so. I sit as a Met lead, but also link into a national policing portfolio of leads focusing on this area.

Q23 **Dr Gardner:** That is really reassuring; thank you. My actual question is this. In February there was the UK Government phone theft summit, at which it was agreed that there would be greater intelligence sharing between yourselves and the mobile phone companies. Has that happened, and how do you describe your relationship with the mobile phone companies?

Darren Scates: I think we have a positive relationship. We meet regularly. This is how we have developed the asks that I described, through good interaction with them. For example, we have spoken to the network providers to say, "Does the blocking you do in the UK get abused, or are there examples where you see abuse of that?" I don't think that Vodafone would mind me quoting them. They have said that they don't see any significant abuse of the process for the GSMA blocking. We have obviously passed that on as, hopefully, some reassurance to Apple and Google, that they do not see a lot of abuse. Should they block a phone when it should not be blocked, they can always unblock it. It is not a one-and-done process.

We have good co-operation and good communications. In terms of data sharing, we share the IMEI number of every stolen phone that is reported to us. When the IMEI is known to the individual—it is not always—we share that, and it is then available to industry. All the network providers receive that information. We have also confirmed with the GSMA and another organisation called Recipero, which do something similar, that they are very happy to share that with Google and Apple. We have secured that agreement, effectively, to help the cloud providers.

Q24 **Dr Gardner:** Are you happy with your relationship? Is there any intelligence that you are not getting hold of, that you would really like to get hold of and that you would like the mobile companies to be a little bit more transparent about?

Darren Scates: There is ongoing analysis happening by the cloud providers to try to give us more detail. For example, we spoke earlier about phones going abroad. Some are probably being broken down for parts. Some are probably being used as live phones. We know from the street value that it seems likely. We are getting into more detail to understand what that percentage split might be.

Commander Conway: We have a secondary ask of industry as well. The first ask, and the primary one, is the denial of cloud services, as we talked about, as a way of nullifying the value of the phone overseas. The second is returning to an ability to display the IMEI on the device if we find it here in the UK. It probably talks more to Kit's example. If we had responded and were able to catch those guys on a bike down the road, being able to confirm the identity of the phone there and then on the street would mean we could link it back to a victim.

Q25 **Chair:** Darren Scates and Commander Conway, we have one minute left. What you are saying is that you are asking the phone companies, when you give them the IMEI number, to prevent that device from contacting the cloud. You are asking them to display the IMEI number on the phone, but the phone companies are refusing to do that. Is that what you are telling us?

Darren Scates: If I may, Chair, we are actually asking the cloud providers specifically—

Chair: Yes, the cloud providers.

Darren Scates: —to prevent a lost or stolen device from connecting to their cloud services. They have not yet agreed to do that.

Q26 **Chair:** The cloud providers in this case are Google and Apple. It is not Microsoft, AWS or the others. Those are the ones that provide cloud to phones. You have asked them basically to cut off the access of a stolen phone to their cloud provision, and they have refused to do that. Have you any idea why they would not want to stop facilitating stolen phones being used?

Darren Scates: In all candour, they have not given us a final answer, but so far they have not agreed.

Q27 **Chair:** How long have you been asking?

Darren Scates: Since October 2023.

Chair: That is 18 months, and you haven't had an answer.

Q28 **Dr Gardner:** They've got a summit next month.

Darren Scates: There will be another summit, I believe, yes. In terms of concerns that they have, they have, for example, said to us, "What if it is abused?" That is a fair question, which is why we then went to Vodafone, which do the UK blocking of the network, to ask that question: "Do you see any significant examples of actual abuse of that system—people getting someone else's phone blocked?" It might be a coercive relationship or some kind of issue around that. Vodafone tell us that they do not see any significant examples of that and that, if it happened, they could then unblock the device. We have obviously provided that to the cloud providers as reassurance so that they can consider further.

Commander Conway: A bank card is cancelled when it is stolen, and it can be uncancelled when it turns out—

Chair: Sometimes that may be done in error, or you may find it, but it is worth having the opportunity to cancel it in order to prevent all the negative consequences of having a stolen credit card. We have to end the session there. Thank you so much; it has been really interesting.

Examination of witnesses

Witnesses: Dion Price and Katarina Zotovic.

Q29 **Chair:** Welcome to the second panel in the Select Committee's one-off inquiry into phone theft. We have heard from the Met police of the serious consequences and the level of phone theft, particularly in London but also across the country. I am going to ask our industry technology experts to introduce themselves as they answer my first question. What are the current available tech solutions to phone theft? How widely are they used by customers? Could you talk a little bit about the barriers to

the adoption of these solutions?

Katarina Zotovic: Thank you very much, first, for the opportunity to be here and to speak about this. As a brief background, I did my master's in criminology at the University of Cambridge before joining S-RM in their digital forensics team. We routinely perform forensic preservation and analysis of digital devices—typically, computers and smartphones, as well as online accounts. My speciality has been smartphone-based evidence. Alongside criminal and civil cases, we work with private clients proactively to secure devices and accounts from threats, reputational damage, IP theft and financial fraud. We have reactively worked with private clients as well to help them regain access to their accounts after mobile phone theft. That is the angle I approach this from.

In terms of what is being done currently, it is important to address that there are great measures in place by top manufacturers. Before I get into those, I want briefly to discuss what I think are the top three prongs, or drivers, for mobile phone theft. The first is user data. More individualistic or smaller groups of criminals shoulder-surf in bars to try to get the PIN of a device, and when you leave it on the table they snag it and get full control of your phone. They can transfer money and gain full access to your handset. The second is thieves, maybe more en masse, who want to try to remote wipe, or completely wipe and reset, a device, to sell it as a whole. The third part is components. Those are the three main targets.

Top manufacturers have thoughtfully designed and implemented measures specifically around the data side. We see remote locking, wiping and device tracking, which I think is what consumers most commonly know and use. They have also been implementing more and more theft detection and tamper alerting, to try to combat the issue further.

On the hardware side, we see more component serialisation. Apple has introduced, with iOS 18, the serialising of parts of a device to the Apple account tied to the device. My understanding of that feature is that if the components are put in a different device they are still technically usable—their functionality is just a bit degraded—so their value would be limited, but not completely wiped, and it could still be of use. Those are my overarching thoughts on manufacturers' measures that exist currently.

Q30 **Chair:** Thank you very much. Dion Price, we heard a little from you earlier, but what are the currently available tech solutions, and what barriers do you see to their adoption?

Dion Price: In addition to the summary that we discussed earlier, one of the main things that comes out of these kinds of review, from our perspective, is a lot of frustration, frankly. We solve this exact problem today, for 70-plus companies: they are mobile phone operators, retailers and financiers. We do that across 35 countries. The incentive is financial. If you are buying, in many cases, billions of dollars-worth of devices in a given year, and moving them around, you need to protect them in the

supply chain, and you need to protect them if you are financing them. If you have allowed someone to walk out of your store with a $1,000 smartphone and they have given you only $100, you'd better have a way of making sure you get the remaining $900, if you are doing that across countries where you have tens or even hundreds of millions of consumers.

To Katarina's point, the locking technology that already exists with all the phone manufacturers today is more than good enough. We use it. We stitch together about 11 different locking technologies. They are all slightly different in the way they are implemented, but clearly Apple has MDM-based solutions; Google has something called Device Lock Controller that works within the operating system on Android; Samsung has something called Knox Guard; Motorola has something called Moto Safe and so on. We stitch all those available locking technologies together.

The main point there is, what is different? Why is there a problem to solve in this country, and why is it a criminal problem rather than a financially motivated one? It is frustrating because when there is a significant financial incentive to solve a problem, lo and behold it is solved. That is why we exist. We get that solution right now, in anger, in 35 countries, and we are, dare I say it, pretty good at it, otherwise our enterprise would not exist. The technology exists, and they do a very good job of implementing it and pouncing on vulnerabilities as they appear and as criminal enterprises start to hack around them.

Unfortunately, the system in the UK, where you try to lock post theft, is closing the barn door after the horse has bolted. In many instances the locking technology is user opt-in. There are several layers to it, and not everybody is even aware of that. Further downstream you have multiple problems, because a number of people turn off the GPS on their phone, which makes it impossible to track. There is PIN security, and a whole bunch of fallibilities and chinks in the armour further down the track, because it is not an automatic opt-in system.

The way we solve that financially is that, as soon as we receive the manifest of millions of devices, they ship with the IMEI. The IMEI is the lingua franca of shipping mobile phones around the world. That is how they are moved and how you identify them, in every incident. Our colleagues here today from handset manufacturers will know every IMEI that is docked into this country. So does HMRC. That is how they are governed, not just for security purposes; it is how they are tracked. We ingest all of those into the system for our customers, who lock them if there is an issue and they are stolen in the supply chain. We have customers in certain countries where people take a bulldozer to the back of the store, rip a wall out and steal all the devices. Because we are now able to lock those before they even hit the storeroom, the incentive has been designed out and that style of theft is—

Q31 **Chair:** To clarify, you say you lock the devices before they are in the storeroom. You lock all the devices remotely using your knowledge of their IMEI numbers.

Dion Price: They are technically in a state called "ready to lock". All the IMEIs sit in our system and are ready to lock as soon as we receive the trigger from our customer: "We were shipping it via a courier to someone's house and it's gone missing; the courier driver says he can't find it. Here's the IMEI. Please lock it." That is an API-based system. It is automatic. There is no phone call. If somebody has stolen an entire lorry-load of devices: "Here's the manifest of IMEIs. Can you lock them all?" Yes, no problem.

Q32 **Chair:** Can you put your personal phone, or can I put my personal phone, in that ready-to-lock state?

Dion Price: You have to capture the devices at the first turn-on. Because devices that are on the street right now have never been registered in any of those systems, they are subject to the locking technology that we have in the market today. We receive manifests of IMEIs and ingest them into the system. Throughout the entire life of the device, no matter what happens to it, if we get the signal from its legitimate owner, we can lock it or unlock it in 30 seconds, anywhere in the world.

Q33 **Chair:** That is your solution. Can I ask each of you what security features, if any, you use on your personal phones to prevent them from being stolen and used?

Katarina Zotovic: It is a great question. Following on from what Dion said, a lot of current features and security measures are opt-in, rather than opt-out. I have an iPhone, for example, and I use stolen device protection. I went into my settings and turned it on. I have my cloud account Find My all enabled and activated. I have biometrics on all my secure applications—as opposed to, for example, a PIN. I just have stronger barriers to entry for user data, specifically. In terms of reselling of parts, for example, I don't have any control over that right now on my devices.

Q34 **Chair:** Thank you very much. Are there any other measures that you use, Dion?

Dion Price: All of that, but obviously my phone is ingested in our system anyway. As you say, we do not install anything on the device. We just use the locking technology that already exists.

Q35 **Chair:** It is already there. Finally, you said that a lot of the anti-theft technology that is based on GPS will not work if GPS is turned off on the phone. Is that right?

Dion Price: If there is any signal that drops down on to the device, whether that is wi-fi or cellular, we can communicate with the modem and lock or unlock it in 30 seconds, wherever it is.

Q36 **Chair:** That is for your solution, but Find My phone and other locking techniques are dependent on GPS and will not be effective in airplane mode, for example.

Katarina Zotovic: Not fully. Apple uses Bluetooth low-energy, which is a kind of mesh technology. Mesh technology allows devices to communicate with one another when they are off of airplane mode or off of Bluetooth, in so far as they are not in, let's say, a Faraday bag, when they would lose all signal, Apple has started rolling out this form of mesh technology to try to allow your devices still to communicate when Bluetooth or airplane mode is turned on.

Q37 **Chair:** That is Apple, but Android/Google does not have that facility.

Katarina Zotovic: Not to my knowledge, right now.

Chair: Thank you very much. I will ask Adam to continue.

Q38 **Adam Thompson:** Thanks, Chair, and thank you both. Good morning. You have talked extensively about the pretty wide array of options available to consumers for anti-theft, but do you think that consumers are broadly aware of those options?

Katarina Zotovic: No. I think user awareness is a huge issue. A lot of features, as we have discussed, are unfortunately opt-in rather than opt-out, and users are not aware that they exist. There are two issues. One is that I do not know that users fully understand the severity of the crime—that phone theft is not just a physical crime and that a cascade of financial fraud, extortion and IP theft can happen as a result. If people were fully aware of that, perhaps phones would not be left on pub tables in the carefree way they are.

The second point is that quite a lot of features are not enabled because users are not aware that they exist. If manufacturers email to say, "Here is a new feature," those tend not to be fully recognised. Typically, with updates on phones, people read more about the new emoticons and aesthetically pleasing features, rather than the new security features to protect the device. I do not think there is huge user awareness.

Q39 **Adam Thompson:** Thanks. Dion?

Dion Price: My reply—I suppose a slightly obtuse one—would be, "Why should they have to?" Ultimately, no one in this room understands how the immobiliser on their car works, and nor should they. You do not opt into the immobiliser settings and have it lock your car in various ways. When more onus is put on the consumer to check various boxes and go into settings, we always say, "This has to pass the grandmother test." It clearly doesn't. That is why we advocate a national IMEI-based opt-out system, so that they are opted in by default as they come into the country. If you are getting consumers to occupy their already overcrowded minds with turning on various settings every time they buy a new phone, you are only ever in a law of diminishing returns.

Q40 **Adam Thompson:** Brilliant. Thank you both for that. I was going to say next, "What is the solution?", but you have been very clear that the solution is an opt-out system. Katarina, you raised an important point about education, but, Dion, you are right: it is very unlikely that most people are going to learn this. It is pretty clear that the solution is an opt-out system, but what barriers do you see between where we are now and all the phone manufacturers bringing in an opt-out system?

Dion Price: Ultimately, an opt-out system requires an orchestration layer. You need one central body. That could be Ofcom, for example, or another Government-appointed body to orchestrate a system. Every device that is brought into the country—obviously we do not manufacture any of them here—is subject to customs and excise, so their IMEIs are registered and logged as they come in. We therefore require a central repository of that information, which already exists. All the mobile phone carriers, retailers and handset manufacturers already use that individual device marker today. It is about collating those together into a central system.

The various locking technologies that exist across different operating systems and handset manufacturers are all slightly different, so there is not one unified solution. They do not all use the same locking technology in the same way. The way we operate, on behalf of the largest, very famous online retailers and very large mobile phone operators, is to say, "Take any phone off the shelf in any stock room and read us the IMEI, and we can lock it for you, if that's what you want."

It really comes down to the barriers. We already solved the problem, so it is slightly more frustrating for us. We do not give too much credence to excuses as to why it cannot be done. Some of our customers buy more mobile phones than the whole of the UK put together, so it is not a problem of size or scale. It is an orchestration problem.

The UK already orchestrates several other things. Each vehicle that is imported comes with a VIN. They are all logged. With firearms every serial number is logged. Medications, explosives, rough-cut diamonds: it is all logged as it comes into the country, on a per-item basis. Tobacco: every single packet of cigarettes is logged, because in the '70s and '80s there was a huge problem with people bringing in cigarettes and selling them, and with HMRC not getting the duty. Those systems already exist. It is an extension of what already happens.

Q41 **Adam Thompson:** A final question from me—a political question, really. Is there going to be pushback from phone manufacturers or other bodies? What is your perspective on that?

Dion Price: From our perspective, we work with them, and have been working with them for over a decade, so we solve the same problem, in the same way we advocate. They do not have to do anything different. All the locking technology that they have right now—at this very second—is what we use. We do not use anything else. The orchestration layer and

pulling it all together is incredibly difficult, which is why we exist; but in terms of pushback from handset manufacturers, if it is a two-way system where you can lock and unlock very quickly and you make sure it is not open to abuse, and you do not have to report a stolen device in a different way—which you don't—then who is to complain?

Q42 **Kit Malthouse:** What is the cost?

Dion Price: The cost is an intermediary layer—an orchestration layer. However you want that to happen—

Q43 **Kit Malthouse:** Well, someone is paying you.

Chair: Someone is paying for that.

Dion Price: That's right, yes. We work for mobile phone carriers or talk to the likes of the largest online or offline retailers. When we are not in the system, we have some customers—take one in Mexico, for example—where delinquency, fraud and theft was 35% of all the devices that they were financing. We bring that down to less than 1% over a period of 18 months.

Chair: That is one organisation that can pay, but we would have to look at the matter of payment.

Q44 **Adam Thompson:** If it is so easy, why haven't we done it already?

Dion Price: It is what we have been advocating. We are solving the problem from a commercial perspective, and in various countries the consequences of phones being stolen are a lot more severe than in this country. We deal with 35 countries, and they are not the safest places to have your mobile phone stolen.

Q45 **Kit Malthouse:** But why not the UK, is the question. Just inertia?

Dion Price: We are very happy to do it tomorrow, if that is what you want to do.

Chair: Clearly, there are costs associated with this. Steve, do you want to come in?

Q46 **Steve Race:** Yes, can I put one question to each of you? Dion, can you be very clear about what happens to a phone after you have locked it, in this opt-out system? It can be broken down for parts, so no one can—

Dion Price: Correct.

Q47 **Steve Race:** Can that phone ever be used again in any way?

Dion Price: Yes, absolutely. It is a two-way system, so it is lock and unlock.

Q48 **Steve Race:** No, sorry, without—

Chair: If it is locked.

Dion Price: Oh, I see what you mean. No. If you are breaking it down for parts, obviously we cannot do anything about that. We estimate that about 7% to 9% of stolen devices around the world go into that ecosystem. A screen can be several hundred dollars, for a top-end iPhone; but if it has been locked in the way we lock it, leveraging all the technology that is there today, the locking technology that my colleagues behind me have in the system is extremely strong, so no, it cannot be used again.

Q49 **Steve Race:** It cannot be used for anything.

Dion Price: No. It is bricked so, in effect, all you have is a screen that says, "This device has been locked." The way we work it for our customers is that if the end consumer has a query, there is usually a number that they can ring—whoever is financing the device or owns it—and they can deal with it.

Q50 **Steve Race:** Just one for Katarina. From a criminology background, what we are discussing is essentially a balance between a criminal element and a technological solution. What is your view of where we should sit on this?

Katarina Zotovic: That is a great question. The angle that I approach it from is the costs element that we have been discussing—for security measures generally to be cost-proportionate. There may be an interesting perspective from the criminological side, as there is a lot of emphasis on making phones less valuable. That is a very rational choice kind of perspective. The idea is that, when thieves weigh the costs and benefits of the crime, if we lower the value it will disincentivise the crime. I fear that there is some income elasticity in crime that drives a lot of organised crime groups, where they have such demand that lowering the value will instead just make them want to increase the volume of phones they steal. There is some solution, when thinking of how these crime groups operate, from a criminological perspective. Maybe it is not necessarily just lowering the value, but completely diminishing the value of the phone. That is what Dion's solution proposes, which I think is great.

One of the barriers is a cost-proportion element. I obviously do not have as much knowledge as the manufacturers do, for example, but phones are already quite expensive, and you do not want to make phones so secure, in such an expensive way, that you outprice the average consumer and end up with a bigger threat landscape, where people do not upgrade their devices as often, so you have more legacy devices—historical devices with older security measures—and then more threats. There is a challenge because at the end of the day the consumer bears the cost of all the development and new technologies that we implement.

Chair: That is very helpful. It is an important point. We clearly need a better understanding of what costs might be associated with an orchestration layer and associated solutions. You have inspired a lot of interest from the Committee. We have only five or six minutes left.

Q51 **Martin Wrigley:** Post theft, post sale, once a device has been acquired by somebody else, in another country or wherever it may be, who is profiting from that situation, ongoing?

Dion Price: An unlocked device, so that it is ready to sell?

Q52 **Martin Wrigley:** I am not talking about your protected devices, but ones that have been sold on somewhere else. Who is profiting?

Dion Price: That is probably a question more for our Metropolitan police colleagues, because they obviously break down the entire supply chain, but there is—

Q53 **Martin Wrigley:** Not in terms of the theft or the shipping; I am not talking about that portion of it. Once it is in somebody else's hands, who is making a profit from that?

Dion Price: Clearly, whoever sells the device on to the new end consumer is making a profit. However, when you go into an Apple ecosystem you generally attach it to various services that sit within it, so if you want to leverage any content that sits on that device—any services, cloud services or entertainment services—that is obviously a revenue stream. The same goes from the Android perspective. The way you monetise that does not necessarily have to be through a credit card. You can use direct carrier billing, so you can purchase various content on the device and it will come off your prepay top-up or be on your mobile phone bill.

Q54 **Martin Wrigley:** So the manufacturers, Apple and Google, continue to make profit. They continue to sell more phones, because these phones are not removed from the system.

Dion Price: Every live phone will make them money in some way, shape or form, yes.

Martin Wrigley: Thank you.

Chair: A very interesting point, Martin. Perhaps we should also look to understand the value of the replacement phones and whether a significant proportion of that is paid for by insurance companies, and understand where the financial incentives, which you set out so well, Dion Price, currently lie.

Q55 **Dr Sullivan:** Following on from that, the police ask was for phones' IMEI numbers to be locked, and access to the cloud thereby denied. Obviously, they have been waiting for that for quite a while. Will that help to solve the problem?

Katarina Zotovic: I don't think that would be a sole issue. The manufacturers already have cloud-based locks, so it would be a kind of second layer of protection. On certain devices, you can also side-load applications. You can get around those a bit. Is it a helpful measure? Yes.

Would it give us that kind of step change in mobile phone theft? I don't think so.

Dion Price: From that perspective it is another hurdle. It is more awkward. To Katarina's previous point, it diminishes part of the value. There are workarounds. You need something ultimately where it doesn't matter if you wipe the device, reset it, install new software or reflash it: the hardware locks, and the locks that we are talking about, that they already leverage, sit at the chip layer. As soon as you power the device back on, the first thing it does, even before you see the home screen, is that it has already called to a system that says, "Here's my IMEI. Have I been stolen? Do I need to be locked?" "Yes, you do." By the time you see the welcome screen, the phone is locked. It doesn't matter what you do to it afterwards: it remains locked forever.

Q56 **Dr Sullivan:** My last question: we are legislators, so do you have an ask for us, or is it a case of the private Apple and Google, the manufacturers, needing to do this? Is there an avenue that we can put forward?

Dion Price: I think the avenue would be a Government body that already exists, or one to be set up, advocating a central repository of IMEIs coming into the country. Those manifests already exist. Nothing different needs to happen there. The locking technology that already sits within the devices does not have to change. It is already more than good enough. As you said, it is a Government body mandating, just as with firearms, explosives, medication and all the other things we mentioned, that as they come into the country they need to sit on a central list. Then the police can plug into that and say, "Okay, block this phone."

Q57 **Chair:** How would that address existing phones?

Dion Price: Unfortunately, it doesn't. Devices that are on the street today are the horse that has already bolted, and we are trying to close the door afterwards. However, in countries where you implement this system, we see what tends to happen on an individual company basis and a national basis: when we deploy with one company, the fraud and theft, particularly in the supply chain, moves from that company to the competitors. It generally takes six to nine months before people start to figure out, "I can't sell the devices I'm stealing over here. The resale value is zero. I'm now going to steal them over here." What tends to happen is that all the carriers in that country start to implement a system like this, and it starts to come down in the country; but you have to cover the whole market.

Q58 **Steve Race:** What countries are you talking about? Is there a good example?

Dion Price: Yes, we go from North America, down through Mexico, Guatemala, Ecuador, Brazil, Chile, Colombia, and then we are into South Africa, Uganda, Rwanda, Nigeria, Kenya, Côte d'Ivoire—

Q59 **Steve Race:** With what you were talking about with phone thefts—

Chair: Orchestration.

Dion Price: Mexico is a very good example. We started out with one carrier in Mexico. We now cover all the carriers in Mexico, plus the top two retailers.

Q60 **Chair:** To clarify, you are talking about your commercial solution rather than a Government body that has a central depository of IMEIs, as you have advocated.

Dion Price: That's right.

Q61 **Chair:** Is that implemented anywhere?

Dion Price: No, it is not. You end up with one by proxy. If you end up with the whole market that sells devices today on the same system, by default you have a national system to reduce the problem. The closest thing we found to it is a mandate in California, probably about six or seven years ago, where they were asked to make sure the locking technology in the devices was default turned on. That was a little bit of a sticking plaster, and because there was no orchestration layer, the implementation fell away. There was some initial effectiveness; it dropped the crime by about half but, again, it petered out gradually over time because no one was controlling the system from a central perspective, applying lock/unlock and making sure they stayed on top of the issue.

Chair: Thank you very much. I am afraid we have to end it there, but it has been really interesting. You can see how engaged the Committee has been. It emphasises to me that we are dealing with incredibly smart phones, by definition, and with incredibly powerful and ubiquitous networks and manufacturers, yet we cannot turn these phones off once they have left our possession. That is something we will talk about in the next session. Thank you very much for your contributions.

Examination of witnesses

Witnesses: Gary Davis, Simon Wingrove and Nabil Ahmed.

Q62 **Chair:** Welcome to the final panel in the Science, Innovation and Technology Committee's one-off inquiry into phone theft. We have heard from the Metropolitan police and from technology experts, and we are now going to hear from representatives of the phone companies. I welcome you, and ask each of you to introduce yourself as you answer my first question. How responsible do you feel for keeping customers safe by reducing the incentives to steal devices, and what is your approach to tackling phone theft? A brief summary.

Nabil Ahmed: Thank you very much. Thank you, Chair, for having us here. I head up the technical and services team in Samsung UK. In terms of the topic of phone theft, Samsung takes that very seriously. It is important to give some context on how we fit into the smartphone

industry. Primarily, we are a device hardware manufacturer. All our Galaxy devices come with the Android operating system, with our partnership with Google. Effectively, it is almost like we wrap a skin or a wrapper around it and develop a user interface on top of the operating system, and we add our services and applications to differentiate in the market.

In terms of the phone theft prevention software features that are available, all the core Google features are available on our devices. We add an extra element for more security—sorry, an additional dimension. Let's say we have the identity check software feature. In addition, we add a security delay feature to provide an additional layer of security for the end user. We take that seriously. As a technology company, we are bringing out new software features to prevent phone theft. We recently launched it on our Galaxy S25 devices. At the same time, we are pushing it out as a software update to our existing devices in the UK, going back as far as 2021. That is the technological solution from our perspective in pushing out these features to new users and existing users.

We are not just resting there. We want to drive awareness and uptake of these software features to protect user data. As a result, we are being proactive, and we have already sent out a public message to 40 million Samsung product users in the UK, talking about all these new security features, how to set them up, and then how to utilise them to protect their data. That is going across all our social media channels, our website, our retail staff, and our phone training staff. That is the second part of driving that awareness and the uptake of it.

The third element from our side is partnerships. We want to play our part in working with Government agencies, law enforcement agencies and other tech companies to tackle the serious issue of phone theft.

Q63 **Chair:** To clarify, Nabil Ahmed, you talked about protecting data. Protecting data is not the same as protecting the phone.

Nabil Ahmed: Correct. Yes, sorry, I meant user data and protecting the phone overall. It is on both sides, sorry.

Q64 **Chair:** How do all the measures that you described protect the actual phone rather than the data?

Nabil Ahmed: We have the core Google features, which are theft detection, the remote lock and the offline lock. Theft detection would use the motion sensors of the device and the AI engine. If there is a sudden, sharp movement, it would detect and lock the device. That would protect the phone.

Chair: Those are the features that Google has preloaded on your phone.

Q65 **Emily Darlington:** Does that render the device unusable by anybody else?

Nabil Ahmed: It would activate the screen lock of the device. As a result, if a phone thief has their hands on it, they would not be able to enter the device.

Q66 **Chair:** But those are Google features.

Nabil Ahmed: Correct, yes.

Q67 **Kit Malthouse:** It is still shippable and usable elsewhere. It is still shippable, resettable and usable.

Nabil Ahmed: This is just protecting the phone and the user.

Q68 **Kit Malthouse:** In the moment, but not from what we have been talking about today.

Nabil Ahmed: Correct.

Q69 **Chair:** How many people do you have working on phone theft and protecting the phones from theft, and where are they based?

Nabil Ahmed: In terms of the R&D and software development?

Chair: Yes, the product development.

Nabil Ahmed: We have a security team in our head office in Suwon and various research offices across the globe looking into this matter and working in close partnership with Google.

Q70 **Chair:** Perhaps you can write to us and say how many people are involved.

Nabil Ahmed: Yes, we can.

Q71 **Chair:** Simon Wingrove?

Simon Wingrove: Thank you very much for the opportunity to be here today and to speak. To follow on from Nabil and expand a little bit on those features, it is helpful to consider the journey of a device when it gets stolen. If I unfortunately had my device stolen today, my first worry would be—

Q72 **Chair:** Do you have all the features enabled?

Emily Darlington: And you didn't have it stolen?

Simon Wingrove: Yes, I do, and no, I didn't today, luckily. My first concern would obviously be for the expensive thing that just got stolen, but probably immediately following that I would have a more serious concern that my phone, if it got snatched out of my hands, perhaps was unlocked. There is data on the phone. There is my banking information on the phone. My phone can be used to make contactless payments. The first thing that I would want to do is try to get my phone locked.

Our top priority is considering the user who has been a victim of the crime and the steps we can take to address their problem. A lot of the

features that we built and launched earlier this year, in partnership with Samsung and other people in the Android ecosystem, are around getting the device locked as quickly as possible. The theft detection feature uses an AI model on the device that looks at all kinds of information, including the accelerometer sensor data, to detect whether a snatch-style theft has occurred and lock the phone down. We then built features like remote lock that make it even simpler than it was before to very quickly get your phone, if it was taken unlocked, to become locked so that it cannot be used for things like contactless payments and accessing the data on the device.

We also built other features like offline detection lock. We heard from other people giving evidence today about people putting phones in tin foil or in Faraday bags to take them offline. We thought through the journey of the thief taking the phone. One thing that I might want to do is try to take it offline so that these remote locking features cannot be used. We built offline connectivity detection that detects if the device is taken offline in a suspicious way, and we lock the device down proactively without it even needing to have network connectivity.

To come back to your original question, we consider these technological solutions to be an important part of the overall process of protecting users against phone theft and, ultimately, trying to reduce the prevalence of phone theft. Those newer efforts built on top of the more fundamental protections that we have had in place for a while, including Find My—recently renamed Find Hub—allowing a user to lock and remotely wipe their device after the event of it being stolen, and factory reset protection, which means that if a device is taken and then attempted to be resold, you need to unlock the device and prove that you were the original owner of the device before you can set it up again and use it as a new person.

Q73 **Chair:** We were told that you cannot tell us how many times the Find My device or remote lock has been used in the UK. Can you tell us that?

Simon Wingrove: We collect data about the ways in which those products are used. For Find My, I don't have the data to hand. I can tell you that, for the new features that we rolled out earlier this year—I think they rolled out in January or maybe very late last year in December—we have seen in the order of hundreds of thousands of what we believe are genuine locks, potentially as a result of theft, globally since those features rolled out. That is still rolling out to a lot of new devices, and people need to opt in to those features.

Q74 **Chair:** It would be useful if you could write to us and tell us how many times it has been used, when you have that information. Gary Davis, perhaps you can answer the question about Apple's approach to phone theft.

Gary Davis: Thank you, Chair. I believe you also asked us to say a few words about ourselves.

Chair: Yes, please do.

Gary Davis: I am Apple's senior director of regulatory and legal. I have worked at Apple since 2013. In my former capacity, I was responsible globally for privacy and engaging with law enforcement on many of the features that I am happy to talk to you about here today.

First of all, thank you very much to the Committee for inviting me along. Apple takes this issue extremely seriously. That is why we are here today to talk about it. That is why we engage with the Home Secretary on it. That is why since 2009 we have been working on features to protect our devices when they are in the hands of our users and, crucially, which I believe is the focus of the discussion here, to disrupt and discourage criminals from stealing phones from the hands of our users.

We introduced Find My in 2009. Find My has an uptake of over 90%. We introduced remote wipe shortly thereafter. We introduced lost mode. We introduced stolen device protection, which we have spoken about, and I think we have now already reached 55% uptake—for a feature that we launched just last year, 55% of our users enabling it is a very strong turnaround. It is not a feature that you need to go into settings to enable. We have prompted all of our users because we think it is important that users be given the opportunity to turn it on. However, in turning it on, users have to make a choice. There are some trade-offs associated with it, and we want to make sure they understand those trade-offs. I am certainly happy to talk more about them after a while.

However, it is crucial for us in this space that we continue to work with law enforcement. I certainly agree with the opening session from the Met about how we need to deepen our engagement on an ongoing basis. Since those first engagements, which the Met referred to, in October 2013, we have been standing by to assist law enforcement wherever we possibly can. I will certainly be happy to talk about that in more detail.

Q75 **Chair:** Thank you very much. I am going to ask each of you to write to us with details of the resources that you have dedicated to designing out phone theft or supporting the security of phones. Find My phone is a fantastic feature. I have an Android phone. I have used it many times. I appreciate that you have figures on how it is used. I will also ask you to write to us with regard to that.

However, I have to ask you this briefly. We heard from the Met the desire to be able to switch off contact with your cloud services for phones with a specific IMEI. Speaking as a telephone engineer myself, I don't understand why you cannot do that. Gary Davis, why can't you do that?

Gary Davis: We need to look at that issue in relation to all the protections that we have in place. We also need—

Q76 **Kit Malthouse:** What does that mean?

Gary Davis: Focusing on IMEI blocking might, in fact, miss some of the problems.

Q77 **Chair:** We heard that from the technology experts previously. I am happy to talk about that. We have another half-hour. But it is just the specific issue of why you cannot turn off access to the cloud for the specific IMEI.

Gary Davis: I will explain the issue in a bit more detail. IMEIs are activated. When you turn on your phone and you see a little spinny screen at a point, that is your phone activating with our servers. The phone will check for IMEI as well as some fraud vectors, because people try to pretend a phone is something else on occasions. We then make a decision as to whether to activate the device or not in conjunction with the carriers. We worry—we have had these discussions with the Met, and that is why Darren Scates referenced it—that there is a vector for fraud. The vector for fraud is in it being done maliciously. People looking to block—

Q78 **Chair:** Okay, thank you. We will come back to that. The reason is that you are concerned about fraud. Can I ask Simon Wingrove the same question?

Simon Wingrove: One of the key things that I want to say is that we absolutely have the ability to block the stolen device from accessing the cloud services. The mechanism is slightly different, but that facility already exists. If you go into the Find My device app and you lock or wipe the device, at that point—

Q79 **Chair:** I am doing that?

Simon Wingrove: Yes, the victim of the theft would do that. At that point, the device is locked. Your Google account, which is on there, and gives you access to cloud services like Google Photos, Google Drive, Gmail or any of those things, is inaccessible to the thief.

Q80 **Chair:** You are not actually answering my question. Why can't you block the access of a stolen phone to your cloud services?

Simon Wingrove: Okay, so the phone is stolen and then it gets reset and resold, and why can we not block access? We can. The mechanism is not IMEI- based. The mechanism is Google account-based. If you have a phone that was previously—

Q81 **Chair:** Why can't you do what the Met is asking for, which is to block it on the basis of the IMEI?

Simon Wingrove: The IMEI is a number that, as we know, is connected to the cellular modem of the device. The IMEI is a construct from the carrier space, from the telecom space, and it represents the modem, the cellular service that is being provided to the device. It makes a lot of sense that carriers use the IMEI as the blocking system for stolen devices. The IMEI is the identifier for the business relationship that the

carrier has with the victim of the theft. They go to the carrier and say, "Hey, my device has been stolen." The IMEI represents that relationship. Our relationship with the user is through the Google account. The Google account is how we—

Martin Wrigley: You could do both.

Chair: So you don't want to, basically.

Martin Wrigley: You clearly can do both.

Chair: There is a lot of interest here.

Q82 **Kit Malthouse:** We are not really getting to the nub of what the answer to the question is, Gary and Simon. You are saying you could block on the basis of an IMEI, but you don't because you think there are other reasons you shouldn't. I guess the Met would say that the harm of you not doing it far outweighs the harm that you are saying may occur from those things. Here is the thing I do not understand. If it's nicked, it is my phone even though it's nicked. If I tell you that I do not want it to connect to the cloud, why wouldn't you just do what I ask with my property, Gary?

Gary Davis: I am happy to answer the question in as much detail as you will afford me to do. I mentioned activation lock. Activation lock is a feature that we have had since 2013. It was introduced in 2013 in response to a very similar public concern at that time that devices were being stolen and that phone manufacturers needed to take more steps to discourage it, in pretty much the same way as we are here today. When you place activation lock on a device—we have 91% of users in the UK with activation lock in place—that will prevent the device—

Q83 **Kit Malthouse:** We understand that, but it very obviously is not, because the numbers of iPhones being stolen in London—70% of the numbers being stolen—have been rising.

Chair: Eighty per cent of stolen phones are iPhones.

Kit Malthouse: So it is very obviously not working. Part of our frustration, Gary, and I am sorry that we keep interrupting you, is that the impression that some of us are getting is that you are avoiding answering the question.

Gary Davis: No, I would like to answer the question. In fact, I am not here to avoid questions.

Kit Malthouse: It is a very simple question.

Gary Davis: I want to answer very clearly.

Chair: But you are answering it by talking about other features.

Q84 **Kit Malthouse:** It is a very simple question that we want you to answer.

The user and the police are asking you to prevent this phone from accessing the cloud when it is wherever it is overseas. Why wouldn't you just comply with that wish by the owner of the phone and the police?

Gary Davis: That is an important point that you make there. We are concerned about a world whereby it would be a person who claims to be the owner who is asking. I can see that you are questioning that. We see extensive fraud attempts. Every month—this is an area that I have been responsible for in Apple—over 1,000 people try to imitate you, me and other people here to seek your data from us and to delete your accounts.

Why do they do that? They do it for malicious purposes. They do it in order to then maybe blackmail you. We see these attack vectors on an ongoing basis. I would like to think, in an area such as this, that our expertise built up over time in relation to attack vectors would mean something. However, the police reporting a matter to us is a conversation that we can continue to have. I am not saying that we are opposed to that at all. I would wish to see that assessed in the context of all the other protections that we have in place. I am worried—

Martin Wrigley: You are missing the point.

Gary Davis: I don't think so. If we focus only on activation lock and on IMEI block, we are going to miss the market for parts. We will still have criminals incentivised on this issue.

Q85 **Kit Malthouse:** We understand that. We are not saying that it is necessarily the silver bullet that will stop it all, but it would help. There is no reason, even with the commercial solution that we heard earlier, that this would not still help with other phones.

Gary Davis: I would also like to believe that the Committee would wish to ensure that there was an overall solution. The overall solution requires us to continue to take necessary steps. We have shown that for years. We have not stood still. We have taken steps. Stolen device protection last year was a major update. Activation lock for parts, which I heard Katarina call serialisation, is a major step in trying to discourage criminals from using second-hand parts in the market. It could well be that IMEI blocking is a natural next step. However, I would want to make sure that, as part of all of that, the Met police continue to do traditional policing, which means sending requests to us for stolen devices and Apple responding to those requests for stolen devices. We are not seeing that. It is important—

Q86 **Kit Malthouse:** The Met said they provide every single one.

Gary Davis: Not to Apple. The numbers of stolen devices that we receive—

Q87 **Kit Malthouse:** Gary, here's the concern. The concern is that, actually, it feels to a lot of people like you are dragging your feet and that sitting behind this is a very strong commercial incentive. The fact that £50

million-worth of phones are stolen in London every year means that, if that stopped, £50 million of sales would be depressed. You would also lose the income from the phones that are then reused overseas, which now must run into the hundreds of thousands, if not millions, of stolen phones around the world from which you are benefiting.

You use phrases like, "We stand by," and, "We must continue our conversation." You are one of the smartest technology companies in the world. If there is a security problem with hacking the phone, you turn the patch around in 48 hours. You are able to detect all sorts of clever things about my behaviour, my face and my fingerprint; yet, for what seems to most people like a relatively simple solution to an endemic and significant problem of crime in London and other capital cities, you are saying that you have been at it for 12 years and made no progress. That is why people feel cynical, I'm afraid, about the motivation.

Gary Davis: No, I understand your concern and I understand that you feel the need to express it that way. I think it is a little unfair. It is necessary for me to refute the suggestion that we somehow benefit from our users suffering the traumatic event of having their phone stolen and being disconnected from their lives. That is not something that we want. We have invested many hundreds of millions—far more than that at this point—in designing in protections. That is why last year we introduced stolen device protection, and that is why we have now moved into the market for second-hand parts—in order to discourage it. It is important that I leave you here with this: our company, from the top down, is absolutely committed to taking necessary steps to assist in this space.

Q88 **Kit Malthouse:** I have two final questions. Are you at all concerned that in allowing stolen goods to reconnect to your cloud services you might be exposed to proceeds of crime litigation? Effectively, you are profiting from a stolen item.

Gary Davis: I don't believe we are profiting. That is not something that we have examined with the authorities. We are absolutely focused on ensuring that, whatever the appropriate steps are, we take them. I hope, looking at the broad range of steps that we have taken, and continue to take, as recently as last October, in targeting the market for stolen parts, that we will discourage criminals. These things can take a while to work their way through the market. I am not saying we stand still.

I was encouraged to hear Commander Conway say earlier that we have seen a small decrease. That is encouraging. Maybe those steps are beginning to seep through. We are not complacent in any way. We are focused on whether activation lock is working and doing what we need it to do. If not, we will look at extra steps. Our track record shows that. We are in this together. We need to do that work with the Met police. We need the requests to come to us. We need to give them the responses. They need to use the information that we provide to them in order to identify where the phones have been stolen and therefore, I assume, target resources. I am not seeing those requests come through to us.

Chair: You seem very keen on telling the Met how they should be doing policing. We have identified that there may be improvements, but you seem reluctant to simply do what, as Kit has so powerfully said, your customers want you to do, which is stop the phones accessing the cloud services. That is the impression that you are giving the Committee.

Q89 **Martin Wrigley:** You clearly do a lot of work trying to protect users' data and protect access to services and do all the things that you would naturally do, which you must not stop and you must continue doing. We are not suggesting that anything other than good work has been done. However, you could tomorrow stop phones that are on the GSMA blacklist and IMEI blacklist connecting back to your services if both of you so wished, and you will not do it. Why?

Gary Davis: I don't know if you want me to—

Martin Wrigley: Either of you. You won't do it.

Chair: Simon Wingrove, as you haven't answered.

Simon Wingrove: It is a really good question. I am not saying that we won't do it. What I am saying is that—

Q90 **Martin Wrigley:** You will do it?

Simon Wingrove: Currently, as it exists, the GSMA database is built by carriers, maintained by carriers, populated by carriers, and read and used by carriers. If we want to change that so that it becomes a database that is used by other actors to do other things to devices and to block them in other ways, that is an industry-wide discussion that is not in my power as an engineer at Google.

Q91 **Chair:** Sorry, I just don't accept that. We are not asking for the GSMA to reconfigure its database with IMEI. We are asking Google and Apple not to allow a specific IMEI phone to connect to their services. We are not asking for the reconfiguration.

Simon Wingrove: We need to decide as an industry that that is a safe and sensible thing to do and then be able to ingest that data.

Q92 **Martin Wrigley:** After 12 years?

Simon Wingrove: The Home Office working group that we are a part of is a fantastic forum for us to have that discussion, because it has all the relevant people in it. It has Apple, Google and Samsung. It also has the carriers and the police. I am very open to having that discussion as part of that working group and seeing if a system can be built. I am here as a technical expert from Google. My team built a lot of these theft protection features. My knowledge is primarily around the technology. What I want to for an IMEI blocking solution is to understand technically how it would work, how the IMEIs would get provided, and how safety, privacy and security would be assured.

Q93 **Martin Wrigley:** That is already working. We heard from the police

earlier that that system works pretty well here in the UK, which is why these phones are moved to networks that do not sign up to the GSMA blacklist. You are the central point that can close that gap, which would then stop phones being stolen, of any type or age, on the streets today and being used in some far-off country where they do not implement the blacklist on their network. You could implement it for them over the top. You have put in services over the top. You have disintermediated most of the GSM systems and you have caused the hole to be there, because they can use your phones without that going on. Consequently, you owe it to customers around the world to implement it immediately. No ifs, no buts—just do it.

Chair: Would you like to respond to that?

Simon Wingrove: We absolutely agree that technological solutions form a key part of reducing this problem and that we have responsibility to the customers. We know that features related to phone theft are very well received. We know from market research that users really care about these features and really care about their phones being protected. It is in our financial interest therefore to build more of these features because they attract users and the sale of phones. Phones with these new features on them are attractive. We are definitely not opposed to doing this work. We have built a system that, as we have already heard from other experts today, is robust and works very well. It happens to not be based on IMEI, but that is not to say that we have not been doing the things that we should be doing. We have been trying to build these systems.

Martin Wrigley: That again misses the point. You are solving a different problem. Solving the physical hardware handset is what IMEI is designed for—international mobile equipment identity number. That is the unique identifier of the handset irrespective of the services. You protecting your services is fabulous, great, excellent, but protect the hardware, too.

Chair: I certainly would not say that we had heard that it was robust, given the levels of phone theft that we are hearing about and the impact on society that follows.

Q94 **Emily Darlington:** I will start by saying that my constituents in Milton Keynes and, I am sure, people right across country are going to sigh and say, "What is this session?" As colleagues have pointed out, we have tried to create a session where we can talk about the technology. We get what you are doing on the data side. It has vastly improved. We appreciate that you are protecting our personal data, absolutely, but what we are trying to look at today is how we disrupt the actual market for the devices. I appreciate you saying that the police's request to block IMEIs from reconnecting is something that you will consider. I hope you will do that faster than "consider", and implement it. I appreciate that it is not the entirety of the solution.

Without talking about protecting data, but specifically about stolen

devices, as technology officers and as protection officers, what are you doing to disrupt the secondary market in stolen devices in other markets around the world? I am giving you an opportunity to talk about just that. Please don't go back to saying everything that has been done to protect data. We are talking about disrupting the actual phone theft that is going on every day on the streets in London and elsewhere in the UK. Those phones are going overseas. It is not about my data; it is about the actual device.

Chair: Shall we start with Simon Wingrove?

Simon Wingrove: The primary piece of technology we have that is about the protection of the device rather than the data is factory reset protection. Factory reset protection has been a long-standing part of Android for multiple years. Factory reset protection means that, if you reset a device and you want to resell it, you need to provide your credentials from the previous owner to unlock the device and make it available for reuse. If the device has been stolen, you cannot provide those credentials and the device is not usable as a device.

It is absolutely fair to say that we see evidence that devices are being stolen and are being reused. We build the software for Android devices. Along with all software that is built, there will be bugs, vulnerabilities and problems. We do not stand still on maintaining that solution. In the most recent release of Android, we announced a significant hardening of the factory reset protection system. In the forthcoming release of Android, we have announced additional hardening of that system. It is a system that prevents the device from being reused after theft unless you are the legitimate owner of that device.

Q95 **Emily Darlington:** But it's not working at the moment. Why isn't it working? When you say you are doing some updates, how many people are involved in that? How much is Google investing in the solution? How quickly can we see a solution on that?

Chair: Just on the specifics of the process, who presents their credentials? You say that the previous owner has to present their credentials. To whom? To Google? To the device?

Simon Wingrove: The device will be locked until, for example—

Q96 **Chair:** So it is a password.

Simon Wingrove: Yes, exactly.

Q97 **Chair:** It can be broken with a password. It is the original password.

Simon Wingrove: For example, it is the user's account credentials. They would need to log into their Google account. That will communicate with the Google service. It is the same protection that would back Gmail or any other solution. Sorry, could you please remind me of the question?

Q98 **Emily Darlington:** Clearly, it is not working. You are talking about an

update. I am trying to understand how quickly people will see these updates. Why wasn't the other one working? How is this new solution future-proofed, ensuring that you cannot do factory reset if it is a stolen device?

Simon Wingrove: The most recent changes to factory reset protection that we have announced were made in the most recent version of Android. I think it is Android 15, if I remember the number correctly. That launched very late last year and is rolling out. How soon can we see the protections? It takes time for Android especially, because Android is an operating system that we build, but we do not provide that operating system directly to the phones. We work with our OEM—original equipment manufacturer—partners, and they integrate that system into their operating system, and then they roll it out to their devices. It can take some time for updates to be available to a wide range of users.

We are really hopeful, because of the efforts that we put in to improve factory reset protection, that we would see a significant impact as that rolls out. We have not stopped investing in that. In the latest version of Android, which has not yet been launched and has not yet been finished, we added additional belt-and-braces-style protection to factory reset protection, working on the basis that we assume that somehow the protection is bypassed—we don't know how—so what could we then do to still block the use of the device even in that situation?

Q99 **Chair:** We don't have much time left. I will ask Gary Davis to answer that question as well.

Gary Davis: I would like to focus on activation lock for spare parts. I know that you do not particularly want us to focus on these issues, but I will say that—

Q100 **Chair:** The Committee is asking you questions. It is for you to answer the questions that the Committee asks, not the questions that you want to answer.

Gary Davis: No, but this is a very important update.

Q101 **Chair:** The question that Emily asked is specifically about the device.

Gary Davis: It is a device feature.

Q102 **Chair:** A device feature. But this is about protecting the actual phone—protecting the whole phone. Is that right, Emily? Please answer that question.

Gary Davis: It is not for data, I guess. I haven't tried at any point to answer about how we are protecting data. The spare parts thing is extremely important.

Q103 **Emily Darlington:** There may be questions from other people on the Committee, if we can get through this, if we have time, about the spare parts. We absolutely appreciate that there is a market for spare parts. I

am asking what Apple is doing to make sure that a device stolen device on the streets of London out of my hands cannot be reused in other countries, that it is being shipped to, as a device. Then we can talk about spare parts. As a device, what is Apple doing to make sure that it can no longer be used?

Gary Davis: I understand. Our best protection is activation lock. I understand you will take the view that it obviously must not be working because there are still devices being stolen, but we have seen a large increase in the uptake of activation lock. That is our strongest protection. You can also place your device in lost mode, which will stop it being activated on our servers as well. A user has various options. Activation lock is a strong protection.

Q104 **Emily Darlington:** Okay, fine. As 80% of phones being stolen off the streets of London are Apple phones, there is clearly a way around that. Is Apple investing any R&D into—

Gary Davis: Absolutely.

Q105 **Emily Darlington:** How much and how soon? What kinds of solutions are you coming up with, and how soon can Apple customers in the UK expect to see those features on their phones?

Gary Davis: Activation lock is something that we need to keep investing in. There may be other updates. Stolen device protection is an update that we launched just last year and was intended to deal with the first category of thefts that Katarina spoke about—the over-the-shoulder thefts that people suffer. There is a strong update in relation to that to discourage the kinds of close personal thefts that people were suffering.

Q106 **Chair:** We are running out of time. It is clear from the mood of the Committee that we do not feel that either Google or Apple has a road map for effective phone protection that does involve IMEI. I think I am right in saying that. The lack of urgency about this subject, given the suffering it entails, is also coming across to us.

In the last few minutes, I have one question, and then I will come back to Adam. You mentioned, Simon Wingrove, that you wanted to end phone theft because people would want to buy more Android devices. You have 52% of the phone market worldwide. I think Apple has 48% of the phone market worldwide.

Gary Davis: I don’t think that is quite right.

Q107 **Chair:** What figures do you have?

Gary Davis: I think it is less.

Q108 **Chair:** Let us have the figure. You are a duopoly, effectively. What evidence do you have that people are changing which operating systems they buy based on the security?

Simon Wingrove: First, just to give my background, I am a software engineer at Google. I understand a lot about the technologies that we have built. I am not a market researcher or a product manager, but I am aware of the market research and user research that we do before deciding to build features. My team has built a lot of phone theft protection features recently, so it is definitely something that I am personally very passionate about and that we have been working on extensively for a long period of time, driven by user research. The user is saying that this is something that people really care about. We have evidence from market research that phone theft is one of the highest priority security, privacy and personal safety features.

Q109 **Chair:** We are running out of time. My question is about people switching. You said that you had financial incentives to improve the security, but I don't see those financial incentives if people are not switching because of the security, and you have the financial incentives of all the phones that are being bought because phones are being replaced. You are not telling me that you have financial incentives to make the phones more secure. Gary Davis, are you seeing evidence of people switching phones because of security?

Gary Davis: Apple has made security and privacy a major brand differentiator over the last 15 years. We are very focused on ensuring that users, when they think of security, including device security, think of Apple. We would like people to be able to make decisions and to move to the Apple ecosystem based on security, including their device.

Chair: Okay, I will take that. We will try to go for five minutes. I know, Nabil Ahmed, you have not had the opportunity to say very much. The focus has been on Apple and Google. We have a minute each for Adam and Lauren.

Q110 **Adam Thompson:** Thank you, Chair. I want to talk about the features that you have on your devices. You talked with great pride at various points through the session. Nabil, you opened by talking about how you have made a lot of effort to educate people about the features that you have available on your devices. Gary, you talked about 90% uptake of Find My and 91% of activation lock—you repeatedly talked about that. We heard from the previous panel about how there is no opt-in for an immobiliser on my car. I do not need to know how that works. I do not need to understand that in any way. If you are so proud of these features and their uptake, why are they not opt-out by default? Why are they not just functioning all the time and we don't need to know about them?

Chair: We will ask Simon, Gary and Nabil to answer that quickly.

Simon Wingrove: Sure. A lot of the features are on by default. The factory reset protection that we talked about earlier is one of the key ways of locking the device post theft and making it not be reused, and it is on by default. Access to Find My device, which is now called the Find Hub, is also on by default. Out of the box without any set-up, as long as

the user has added a Google account, they can use that Google account to log in, lock their device, wipe their device, and factory reset protection will protect their phone.

Some of the features that launched earlier this year and that I talked about earlier are not on by default. I will give you an example to explain why. One of the features that I talked about was offline connectivity protection if the device gets put in a Faraday cage or wrapped up in foil. If you live in an urban area where theft rates might be higher and connectivity is really good, that is a pretty good feature to have; your device is not going to go offline regularly all the time and you have a risk of theft. If you live in a rural area, where maybe your connectivity is not quite as good and your risk of being a victim of phone theft might be lower, that particular feature might not make sense for you.

It is a case of looking at each of the features individually and working out whether it makes sense for them to be default on, considering it from the perspective of every conceivable user globally, and working out which ones should and should not be default on. Definitely, some of the core protections are default on, but we have also to balance the protection against the user experience.

Q111 **Chair:** Do you have a series of questions when somebody buys a phone and one of them is, "Are you in a rural environment?" Do you have a security procedure?

Simon Wingrove: We have onboarding flows when you—

Q112 **Chair:** Onboard?

Simon Wingrove: Sorry, when you turn on the device, you get a sequence of screens that help you set up the device correctly. We try to use those screens to encourage people to turn on features if they are the right features for them.

Gary Davis: It is going to be pretty much a similar answer. Your user needs to know certain things about how the phone behaves if something goes wrong. I would love for stolen device protection to be turned on for everybody in this room with an iPhone. Before you turn it on, though, you need to know what it means. It means that the phone will behave in a particular way when it is at home or work. It will behave here because it knows that it should be here. It will behave differently if it is somewhere that it is not normally. The user needs to know about that so that they know how to unlock it. In my wife's case, she dropped her iPhone on the ground a few weeks ago, hit a pebble and disabled somehow the face ID camera. Without the face ID camera, that phone was going to remain locked for her unless she went home. She had to go home so that she was in a familiar place. There needs to be an engagement with the user so that we get the balance right.

We are thinking about these things the whole time. I definitely want to leave you with the clear view that we are absolutely focused on ensuring

that the devices are protected to the best of our ability, including if they get stolen, and discouraging criminals from doing that. I know you are concerned about that. It is unfortunate that you have that feeling. However, I hope it is clear through our track record over many years that we are not sitting still. We are working and making updates.

Q113 **Chair:** Your track record over many years means that 80% of phones stolen in London are Apple and 80,000 phones have been stolen.

Kit Malthouse: Fifty million quids-worth a year.

Gary Davis: I don't know if those numbers are right. I also heard Commander Conway say that it could well be that users report Apple devices more. We obviously do not know.

Q114 **Chair:** It is more expensive, but yes.

Gary Davis: It could well be, but we don't know that.

Q115 **Chair:** That could well be. Sorry, let us not get into that. We have a few more minutes. Shall we ask Nabil Ahmed to speak? Then I can come to you, Kit.

Nabil Ahmed: Sure. From a Samsung perspective, we strongly encourage our users to set up their security credentials. As my colleague said, it is part of the out-of-box experience. When the device first sets up, there are screens that prompt the user to set up their security credentials and inform them. We strongly encourage that. It is done right from the beginning. However, we need users to make an informed choice on what features they want to be turned on or off. If you are in a rural area, as Simon mentioned, that might be a concern. There are users who do not want to share their biometrics, such as fingerprints or face ID, for privacy reasons. There is also user behaviour. They will just skip through the settings and start using their phones. There are some users who are a little bit fearful of technology. Even though it is intuitive and simple, they will just skip through those settings. We provide the screens for them to make an informed choice and select those features.

Chair: Thank you, those are important points. You are emphasising, certainly to me, the challenge in putting it on the user to define their own security levels, rather than the ability to turn the phone off from the cloud once it has been stolen.

Q116 **Kit Malthouse:** On the IMEI blocking issue specifically, who is it in your organisations, Gary and Simon, who would need to take the decision? Who is the individual person who would have to say—

Gary Davis: I think I said maybe at the start that this issue has the attentions of the most senior people in Apple. That is the case.

Q117 **Kit Malthouse:** Who? Who would say "go" or "no-go" on blocking IMEI?

Gary Davis: That is a Tim Cook/executive team-level discussion. We are having those discussions. About 25 minutes ago, I answered a question

where I said that we were considering how we would enable IMEI blocking, but it got somewhat lost in the movement that took place. I gave that answer very deliberately. I would not close the door on it whatsoever. I just want to make sure, as we do it, that when we do it and how it is done also takes account of other threats in that space, and that we, all together, in trying to solve this problem, actually solve the problem.

Q118 **Kit Malthouse:** I understand. It is a Tim Cook decision.

Gary Davis: It is one that the most senior people in Apple are aware of and are considering.

Q119 **Kit Malthouse:** Okay. Simon?

Simon Wingrove: I honestly would not be able to give you an answer on how far up my management chain I would need to go to get something like that signed off.

Kit Malthouse: Let us know. The point is that there is an accountability issue. We want to know who in the organisation is taking accountability for this extremely alarming issue in the capital and, indeed, the rest of the UK. We need to be able to pin that on an individual. So it is Tim Cook, and, Simon, you will let us know.

Q120 **Martin Wrigley:** I would just like to thank you because you have both now said that you can stop this by blocking IMEIs on the GSMA/IMEI blacklist, and you are just deciding not to do so yet.

Gary Davis: I think you have presented a slightly different twist.

Q121 **Chair:** Gary Davis, you have mentioned a number of times the chips and the parts. We said that we would come back to that. What is your evidence? The Met told us that they believe that the vast majority are being sold intact. Does Apple have data that that is not the case? Could you send it to us?

Gary Davis: We have seen significant recycling or reuse of what we believe to be stolen parts in the chain, and we want to stop that, yes.

Q122 **Chair:** Could you share that evidence with us?

Gary Davis: We can share that with you.

Chair: Excellent, thank you.

Q123 **Dr Sullivan:** I have a very similar question to what I put to the tech people. As legislators, how can we help? Do we need to help your bosses come to the realisation that we need this level of security, or is it a case that we just let you guys carry on and hopefully the criminals don't win? At the moment, it feels like they are.

Chair: Lauren, that is an excellent question. Can I build on that? Do you have an understanding of how much the orchestration layer that our

previous witnesses talked about, which would enable all IMEIs to be identified when stolen and to be blocked, might cost your company in order of magnitude?

Gary Davis: That is not a proposal that has ever been suggested to us by the authorities here in the UK—never by the Met or anybody else. There may be some commercial interests there. It is not something that we have been asked to do.

In terms of legislators, I have found the engagement with the Home Secretary's summit to be a very useful way to have a conversation. I know you do not want me to make suggestions on how to further improve information sharing with the authorities, but it has been a very useful forum to identify where there were gaps and where we could assist and provide information to the authorities. It is key that we have that opportunity to provide information that is in our possession to the authorities. We need lawful requests to do that. When we receive those lawful requests, we will provide that information. Beyond that, I would like to leave it to that forum to do so.

There is no question of needing to assist my bosses with looking at this issue. I want to be very clear: we are engaged in this at the most senior levels of the company. We feel accountable. We want to ensure that this issue is resolved. The only hesitation you have heard from me today is a concern on my part that if we all focus on IMEI blocking, we will miss dealing with other issues. I hope that is clear from the information that I have put before you.

Simon Wingrove: I agree with a lot of that. I would like to see the GSMA involved in the discussion about the orchestration layer and IMEI blocking. The GSMA owns and maintains the data on the IMEI blacklist. It would definitely be a part of that.

In terms of other support and what can be done to help, I found the Home Office working group led by the Home Secretary to be an extraordinarily valuable thing for being able to have frank discussions and, personally, as somebody who is building these products, to be able to understand how they are being used, how phones are being stolen, and ways in which we could potentially, therefore, improve them. Learning how the theft patterns happen has been immensely valuable for me.

We mentioned that a lot of our features are default on, but some of them cannot be default on, for various reasons. We would like to encourage people to turn those features on, where it makes sense to them.

Regarding other ways that public authorities can help with that, I point to the recent engagement that we had with the Mayor of London, who looked at those features. We gave him a demo. He was then able to promote to Londoners specifically, "Hey, these features exist. You should turn them on. It makes a lot of sense to you." That kind of support is

very valuable as well. I built those features. I would love to see them on as many people's devices as possible.

Chair: Thank you. That is very helpful. You have certainly engaged with our questions very actively for the last hour, and we are immensely grateful for that. I hope you accept that the enthusiasm the Committee has shown for practical answers reflects the views of our constituents and the experiences of so many, and of far too many Londoners in particular.

While we have had positive discussions about a number of ways in which phones can be better protected, there seems to be some very low-hanging fruit; it may not answer the whole issue, and may not protect every phone in every circumstance, but if you said to most people that perhaps the most valuable thing they possess could be rendered valueless to a thief by the simple act of turning off IMEI registration, they would think that that was quite a good deal. That remains our view.

We look forward to the additional evidence that you are going to provide. We remain incredibly grateful to you for taking the time to be with us. This has been a very useful session on many levels, so thank you very much.