

This Transcript has not been proof read or corrected. It is a working tool for the Tribunal for use in preparing its judgment. It will be placed on the Tribunal Website for readers to see how matters were conducted at the public hearing of these proceedings and is not to be relied on or cited in the context of any other proceedings. The Tribunal's judgment in this matter will be the final and definitive record.

**IN THE COMPETITION**  
**APPEAL TRIBUNAL**

Case No: 1403/7/7/21

Salisbury Square House  
8 Salisbury Square  
London EC4Y 8AP

Monday 27<sup>th</sup> - January 2025

Before:  
Ben Tidswell  
Dr William  
Bishop  
Tim Frazer

(Sitting as a Tribunal in England and Wales)

**BETWEEN:**

Dr. Rachael Kent

**Class Representative**

v

Apple Inc. and Apple Distribution International Ltd

**Defendants**

---

**A P P E A R A N C E S**

Mark Hoskins KC, Tim Ward KC, Michael Armitage, Matthew Kennedy, Antonia Fitzpatrick,  
(Instructed by Hausfeld & Co. LLP) On behalf of Dr. Rachael Kent

Marie Demetriou KC, Brian Kennelly KC, Daniel Piccinin KC, Hugo Leith, Hollie Higgins  
(Instructed by Gibson, Dunn & Crutcher UK LLP) On behalf of Apple Inc. and Apple  
Distribution International Ltd

Monday, 27 January 2025

(10.30 am)

DR WENKE LEE (continued)

Cross-examination by MR KENNELLY (continued)

THE CHAIRMAN: Good morning, Dr Lee, Mr Kennelly.

MR KENNELLY: Good morning, sir, good morning, Dr Lee.

Dr Lee, we are moving on to security features and benefits, and your evidence in broad terms is that in distributing apps created by third parties, Android and Microsoft already provide security benefits which are comparable or additional to Apple's. Is that correct?

A. Can you point me to that in my report. I would rather answer the question in the context of this case.

Q. Yes, {C2/5/13}.

A. That would be my report 1?

Q. Yes. It is the very top of the page. That is the end of paragraph 16.

"Developers and consumers of digital content distributed and paid for via other digital content platforms, already enjoy what I consider to be comparable (or additional) security benefits to those offered by Apple and the App Store."

A. (Pause) Yes, that is what I said, yes.

Q. But if there is a difference in security benefits, you say that is not caused by the existence of third party

1 app marketplaces or developers distributing directly on  
2 those other platforms?

3 A. So, again, where do I put it in my report?

4 Q. No, that is in about 20 different places.

5 Dr Lee, just in broad terms, if there is  
6 a difference in security outcomes, your evidence is that  
7 it is not caused by third party app marketplaces or  
8 distributors distributing directly; is that right?

9 A. So in my report I said that the most to me as a security  
10 expert, and someone who has been working in malware  
11 analysis for more than 20 years, my experience is that  
12 no attacker would declare: hey, I am the attacker. So  
13 the most intuitive reason that you should worry about is  
14 that a manufacturer's -- it is different, let us say,  
15 between Android and iOS. I think the most important  
16 factor is that Android does not enforce developer  
17 identification and signed apps.

18 Q. So if there is a difference in security outcomes, it is  
19 not caused by the existence of third party app  
20 marketplaces on Android, is it, your evidence?

21 A. So what I am saying is that there are multiple ways to  
22 look at the differences, right, there are sort of  
23 technical capabilities. In that regard, I do not  
24 believe there is a difference between the technical  
25 capabilities between third parties and, let us say

1 including, Android versus Apple, but there are other  
2 differences to me which are more important. In this  
3 case, it would be policy. Policy means that Android  
4 decides that they allow self-signed apps. That, to me,  
5 is -- when they first announced it I was like, why was  
6 that?

7 There are other factors, such as the fact that they  
8 allow multiple OEMs to do their own devices. So those  
9 are -- to me, it is not a technical contributor to the  
10 difference. At least, that is out of my analysis.

11 Q. Before we look at the data, Dr Lee, do you agree that  
12 security is a question of degree? So what I mean, no  
13 security system is perfect, is it?

14 A. I agree with the definition, there is no ones and zeros.  
15 You cannot say you are absolutely secure, absolutely not  
16 secure, it is always in between. In that regard, yes,  
17 I agree.

18 Q. So the mere fact that a system has not caught malware or  
19 a social engineering attack does not mean it is  
20 therefore a bad system?

21 A. So I said throughout my report that all the app reviews,  
22 including the App Review by Apple and any third party  
23 they tried to detect, for example, detect and prevent or  
24 remove malware. The point I make I think throughout my  
25 report is that nobody is perfect. Also I have not seen

1 a sort of quantitative analysis of the difference that  
2 has resulted from their methods, the technical methods.  
3 I have not seen one.

4 Q. But one way in which we might judge the performance of  
5 a particular security strategy is by comparing how many  
6 successful attacks are levied against that system  
7 relative to another?

8 A. So again, I said this throughout my report including the  
9 joint statement with Dr Rubin here, is that many of  
10 those reports, they only talk about the volumes of  
11 malware you see, let us say, on Android market versus  
12 iOS. To me, like I said a moment ago, when I am wearing  
13 my technical expert's hat I will look at the technical  
14 reasons behind it. I do not believe that just because  
15 you have a higher volume of numbers, that is all due to  
16 technical deficiency. Like I said a moment ago, in this  
17 case a policy has a lot to do with that kind of  
18 difference.

19 Q. Well, let us look at the data on the availability of  
20 problematic apps first and then we will look at rates of  
21 infection.

22 A. Okay.

23 Q. Could we turn up first, please the RiskIQ report. This  
24 is {D1/806/1}.

25 A. Sorry, I am confused. I have different ...

1 Q. It is on the screen.

2 A. You are showing the report, yes, okay.

3 Q. You can see from the cover, it is concerned with the  
4 mobile app threat landscape. Do you see that?

5 A. Yes.

6 Q. This is from 2020. If you go to the bottom of page  
7 {D1/806/2}, please, just to understand what they are  
8 talking about. Can you read the last paragraph on  
9 page 2.

10 This is just -- I am not asking you a question,  
11 Dr Lee, just to orientate to you in this report.

12 (Pause). Do you see that?

13 A. Hang on. (Pause). Yes, I saw that paragraph, yes.

14 Q. Then page {D1/806/3}, please. It continues. Could you  
15 read the first paragraph beginning "These rogue  
16 apps ..."

17 A. Mm-hm. (Pause). Okay.

18 Q. Have you any reason to disagree with that statement?

19 A. I do not disagree what they observe. I disagree with  
20 their kind of causal analysis.

21 Q. Can we go to the next page, please -- the next  
22 paragraph, please, beginning "Many malicious apps ..."  
23 We will come to the causal analysis later.

24 A. Okay. (Pause).

25 Q. In particular, up to "... to keep tabs on them."

1 A. I am sorry?

2 Q. If you read the first sentence, please. (Pause).

3 A. Okay, I read the first sentence of the second paragraph.

4 Q. Any reason to disagree with that?

5 A. So again, I mean, that is how they observe it and count  
6 it, I have no reason to doubt. I myself have not  
7 counted them.

8 Q. Go to page {D1/806/5} in this report, please. This is  
9 looking at, under the heading "Google is Cracking Down",  
10 do you see that passage, it says:

11 "Apple treats its App Store like Fort Knox and  
12 rarely hosts dangerous apps. Google Play's reputation  
13 in this regard is not quite as good. However, its  
14 security controls are improving. Despite allowing  
15 troublesome apps to enter the Play Store at a rate it  
16 finds acceptable, the number of blacklisted apps in the  
17 Play Store dropped an impressive 60% in 2020."

18 Then do you see below that, the figures for 2019 and  
19 2020 for blacklisted apps in the Google Play Store?

20 A. Yes.

21 Q. Have you any reason to disagree with these figures?

22 A. I do not disagree with the figures that they reported  
23 but, like I said, I do not necessarily agree with how  
24 they compare that with iOS App Store or the causal  
25 analysis.

1 Q. We will come to the causal analysis, but do you say they  
2 are wrong when they say that Apple rarely hosts  
3 dangerous apps whereas Google Play's reputation is not  
4 quite as good. Is that wrong?

5 A. Well, I mean, I would just caution you and the panel  
6 that throughout my report I gave plenty of examples of  
7 how the App Store App Review has failed to detect  
8 malicious apps, including my experimental app, the  
9 Jekyll app, which was the first academic example, so my  
10 point is that App Store failed plenty of times.

11 Yes, I mean, by number, Android -- the Play Store  
12 has more, but there are many reasons. One of them  
13 actually is: do you know that Android has twice as many  
14 devices as Apple, iOS devices, the number, they do not  
15 go proportional to the number of devices. If I am an  
16 attacker, I have time to come up with an attack, I want  
17 to hit the biggest target.

18 So, naturally, Android devices which attract more  
19 attacks, plus the fact that they allow self-sign apps,  
20 that, to me, is a giveaway. So my point is there are  
21 many technical reasons that none of these reports either  
22 know or actually bother to go into. They are just: ah,  
23 here is a number. Then they would just draw the most  
24 convenient conclusions. Ah, because they are open  
25 market. There are many differences, many factors. Can

1 I do a better analysis? That is completely lacking with  
2 any of these reports.

3 So, to me, it is completely pointless to use this  
4 report to say, hey, open market's bad. Why?

5 Q. Dr Lee, we will come to the why in a moment. I am just  
6 trying to work out the -- the availability figures for  
7 the moment.

8 You see that the report here says that the  
9 blacklisted -- the number of blacklisted apps in the  
10 Play Store had dropped in 2019 and 2020. Do you see  
11 that? We are still looking at the passage under "Google  
12 is Cracking Down".

13 A. Yes.

14 Q. They say that:

15 "... blacklisted apps have now fallen in Google Play  
16 for two consecutive years."

17 Do you see that?

18 A. Okay.

19 Q. Is it right to infer then that the figure for  
20 blacklisted apps in the Google Play Store in 2018, for  
21 example, was higher than the figure we see for 2019?

22 A. I do not see the figure for 2018, so I do not know, but  
23 ...

24 Q. It says the blacklisted apps number has fallen in two  
25 consecutive years. Just on that alone, is it reasonable

1 to infer that the figure in 2018 was higher than the  
2 figure for 2019?

3 A. Yes, I guess I can trust what it is saying, but how much  
4 higher we do not know, right? It is not in the figure.

5 Q. Blacklisted apps are defined, do you see that, at the  
6 bottom of page 5. It is an app that is already  
7 identified as potentially problematic.

8 Do you see a blacklisted app appears on one global  
9 blacklist, such as VirusTotal.

10 "A blacklist hit ... shows that at least one vendor  
11 has flagged the file as suspicious or malicious."

12 So it has already been flagged as suspicious or  
13 malicious?

14 A. Yes. Again, like I said, (inaudible) is an expert in  
15 malware analysis. I would caution you that when they  
16 say "suspicious or malicious", it is not the same as  
17 malicious. Basically it is suspected to be bad by one  
18 of the vendors, and some of these vendors are known to  
19 have a so-called false positive.

20 So what I am saying is the fact that an app is  
21 blacklisted, this does not mean that this app is  
22 confirmed as malware.

23 Q. It is more risky, though, is it not, if it is on the  
24 blacklist?

25 A. So again, depending on the vendor that labelled it,

1 I mean some of the vendors, they are known to be more  
2 false positives of a certain kind of behaviour, so  
3 I would take a huge grain of salt. Definitely, for me,  
4 from our work, we almost always look at votes by  
5 multiple vendors, not just one.

6 Q. So Dr Lee, are you saying that when an app appears on  
7 a VirusTotal blacklist, it is not likely to be more  
8 risky than an app that is not on that blacklist?

9 A. So then my question is why do they not just say this is  
10 malicious? Why do they say just blacklist it? Or why  
11 do they say only it is suspicious. Why do they not  
12 definitely say, hey, it is malicious.

13 Q. They should wait until they are sure it is malicious  
14 rather than blacklisting it?

15 A. So, to me, they say "suspicious", that means they do not  
16 have sufficient evidence to say it is malicious. That  
17 is -- to me, as an expert, then you take this -- their  
18 recommendation with a huge grain of salt, meaning that  
19 they say something but they do not have full confidence.

20 Q. Moving on to page {D1/806/6}, Dr Lee, and again we are  
21 looking at the leading blacklisted app offenders, and  
22 you see that the most prolific store of blacklisted apps  
23 was in fact the Google Play Store. Do you see that on  
24 the far left?

25 A. Yes.

1 Q. The rest of those are all Android stores, are they not?

2 A. I believe so. They are all either vendors, hardware  
3 manufacturers, or just, you know, Google Play Stores,  
4 yes.

5 Q. Have you any reason to disagree with these figures?

6 A. I do not have -- I do not have reason to disagree with  
7 the numbers, no.

8 Q. You see the Apple App Store is not listed here, is it?

9 A. No, but I would add the following. Google at that time  
10 allowed self-sign apps, 2020. They only sort of  
11 enforced a new policy in August 2021, okay? Also not  
12 only that, they also, in 2021, August, they say from now  
13 on you have to go through our process and then sign  
14 apps, and so on and so forth. Even then, they sort of  
15 went further, the apps that had been submitted prior to  
16 that date.

17 Okay, so my point is up to August 2021, I bet there  
18 were a ton of apps on Google Play Store that were  
19 self-signed. So I am not surprised you see a ton of  
20 these so-called blacklisted apps, whereas on iOS from  
21 day one they insist, developer, identification and  
22 signed apps. Of course, in 2023, like I said, when I  
23 had a security researcher and someone experienced in  
24 malware analysis, I would say, yes, iOS inherently would  
25 have much fewer malicious apps, because simply no

1           malicious app or malware author would declare, hey,  
2           I wrote a malicious app. That is completely  
3           counterintuitive.

4       Q. We are going to come back to code signing and the  
5       causes. I am just looking at numbers at the moment and  
6       asking you to check these figures.

7           Over the page at page {D1/806/8}, do you see,  
8       question 1, there is a reference about halfway down that  
9       paragraph to the fact that five, just five popular  
10      Android apps produce 700 million downloads and accounted  
11      for 353 million suspicious mobile transactions. Do you  
12      see that?

13      A. I am sorry, where am I looking?

14      Q. Halfway down the first paragraph?

15      A. Halfway down the first paragraph. Okay, let me see.

16           (Pause). Okay.

17      Q. You see that these apps had been at some point available  
18      on the Google Play Store?

19      A. Yes.

20      Q. Have you any reason to disagree with these figures?

21      A. No.

22      Q. Now I would like to look at rates of infection,  
23      the degree to which these malicious apps get downloaded  
24      and affect devices. Can we go, please, again looking at  
25      Android in particular, to {C5/246/2}.

1 A. Sorry, is this a report?

2 Q. It is on the screen. It is page 1, please. Show Dr Lee

3 the -- this is about unwanted, it is a study of unwanted

4 app distribution on Android devices. Do you see the

5 report, by NortonLifelock Research Group?

6 A. Yes.

7 Q. If you see -- sorry, the first page, please, still just

8 below the introduction.

9 A. Can you zoom in, please?

10 Q. Yes. Could you read the first paragraph, please, down

11 to "... by default".

12 A. Okay, the first paragraph of the introduction?

13 Q. Yes, just the first paragraph of the introduction.

14 A. Okay. (Pause). {C5/246/1}. Okay.

15 Q. Over the page, please, {C5/246/2}. You see the summary

16 of the conclusions of the study.

17 Now, left-hand column, bottom half, please. Can you

18 zoom in for Dr Lee.

19 A. Left side.

20 Q. So on the left-hand side about seven or eight lines down

21 is a reference to a vector detection ratio. Do you see

22 that, VDR?

23 A. Yes.

24 Q. "... the ratio of unwanted apps installed through that

25 vector over all apps ..."

1           You see the results:

2           "The Play market [that is the Google Play Store] is  
3           the main app distribution vector ... 87% of all installs  
4           and 67% of unwanted installs."

5           A. Mm-hm.

6           Q. Giving it a VDR of 0.6%. Better than the others, but  
7           still significant amounts of unwanted apps are free to  
8           bypass it.

9           A. Mm-hm.

10          Q. Then the second bullet. The alternative markets, the  
11          third party app marketplaces, have 10% of unwanted  
12          installs. They are, on average, five times riskier than  
13          the Play market. It varies, the risk.

14          "Some like Amazon's and Vivo's are almost as safe as  
15          the Play market, but users of other top alternative  
16          markets have up to 19 times higher probability of  
17          encountering an unwanted app."

18          Do you see that?

19          A. Mm-hm.

20          Q. Any reason, Dr Lee, for disagreeing with those figures?

21          A. No.

22          Q. Just the figures, not the causes.

23          A. The figures, no, I do not doubt.

24          Q. Can we please go to {D1/1368/63}, please. This is  
25          a report you relied upon, the Zimperium report. Can we

1 go to page 1 to show Dr Lee the first page.

2 Do you recognise that report, Dr Lee?

3 A. Yes.

4 Q. Page 63, please. Look at the key takeaways. It says:

5 "Historically, iOS devices have faced lower rates of  
6 malware than those encountered on Android devices."

7 Presumably you have no reason to disagree with that  
8 statement? Not about the causes, just the statement  
9 itself.

10 A. I think, by all the reports, it seems to me they have  
11 lower numbers of malicious apps. In that regard, yes,  
12 they are better.

13 Q. Then, please, another document on the rates of  
14 infection, {D1/803/1}. It is the Nokia threat  
15 intelligence report for 2020. You are familiar with  
16 this document, are you not?

17 A. I believe so, but can you like point me to my report.  
18 I want to refresh my memory of the context.

19 Q. I will take you through this document.

20 A. Okay.

21 Q. Go to page {D1/803/7}. Actually, first of all, just  
22 page {D1/803/2} so you see where they are coming from.  
23 Page 2. Tell me, Dr Lee, if this is difficult to read.  
24 I want you to look at the first paragraph, just to note  
25 that they are getting their data from fixed and mobile

1 networks that have installed their protection software.

2 A. Mm-hm.

3 Q. Do you see that?

4 A. Okay, I read the first paragraph, yes.

5 Q. Then page {D1/803/7}, under the heading "Malware in  
6 mobile networks". If you look, please, at the first  
7 bullet point on the left, you see it says:

8 "Over the last few years ..."

9 This report is from -- as I said, it is from 2020.

10 "... a significant improvement has been seen in the  
11 security of official mobile app stores. However,  
12 third-party app stores are still rife with Trojanized  
13 applications."

14 A. I read that, yes.

15 Q. Now, we will come to the causes of why that is, but do  
16 you have any reason to disagree with that statement; not  
17 causes, just that statement itself?

18 A. So again, this is, you know, one report that says so.

19 I do not doubt the numbers, but the conclusion I do not  
20 know. I do not know I agree with it or not. I would  
21 rather see multiple reports discussing that kind of  
22 observations.

23 Q. Let us look at the data on the next page, page  
24 {D1/803/8}. Let us read the text. This is "Infections  
25 by Device", on the left-hand side, Dr Lee, "Infections

1 by Device".

2 A. Okay.

3 Q. I would ask you to look at the third paragraph:

4 "In the smartphone sector, the main venue for  
5 distributing malware is represented by Trojanized  
6 applications. The user is tricked by phishing,  
7 advertising or other social engineering into downloading  
8 and installing the application. The security of  
9 official app stores, such as Google Play Store, has  
10 increased continuously."

11 Then this, Dr Lee:

12 "However, the fact that Android applications can be  
13 downloaded from just about anywhere still represents  
14 a huge problem, as users are free to download apps from  
15 third-party app stores, where many of the applications,  
16 while functional, are Trojanized. iPhones applications,  
17 on the other hand, are for the most part limited to one  
18 source, the Apple store."

19 A. Yes, I read that, yes.

20 Q. Putting to one side the question of why the third-party  
21 app stores have so many malicious apps, do you disagree  
22 with that statement?

23 A. So I mean, that statement basically already talked about  
24 the cause, which I do not agree. Right? They say:

25 "... the fact that Android applications can be

1 downloaded from just about anywhere still represents  
2 a huge problem ..."

3 I mean, that is almost: okay, just because you can  
4 download them from anywhere, that is a cause. To me,  
5 I disagree with that statement.

6 Q. Let us look then, just so you recognise it, the data.  
7 I understand what you say about the causes, Dr Lee, but  
8 do you see the 2019 figures for infected devices, and  
9 you see that the figure for Android is 47.15?

10 A. I am looking at Figure 3?

11 Q. Figure 3.

12 A. Yes, sorry.

13 Q. 2019.

14 A. Yes, okay.

15 Q. For iPhone, it is 0.85%.

16 A. Yes.

17 Q. Infected devices.

18 A. Okay.

19 Q. Have you any reason to disagree with those numbers,  
20 leaving to one side the causes?

21 A. I mean, no, I mean what they report, I trust they do  
22 a good job with the numbers, yes, sure.

23 Q. Then 2020, Android has improved, 26.64%, but the iPhone  
24 is at 1.72%. Again, do you have any reason to disagree  
25 with the figures themselves, putting the cause to one

1 side?

2 A. No, I mean, I trust the adequate numbers, yes.

3 Q. You made the point earlier on, Dr Lee, that there are  
4 more Android devices out there than iOS devices, yes,  
5 you said that to us this morning?

6 A. Yes, twice as many.

7 Q. Twice as many. But the proportion of infections which  
8 are infecting Android devices according to this data is  
9 not double the proportion of infections affecting  
10 iPhones, is it?

11 A. But when I said that, twice as many, I also say that the  
12 number of attacks on the platforms is never  
13 proportionate to the size of that market, which means  
14 that because Android has twice as many devices as iOS,  
15 it does not mean that they only get twice as many  
16 malware submitted to the Play Store. Likely a huge  
17 number of figures, it could be multiple magnitudes'  
18 difference. Because, like I say, intuitively you are an  
19 attacker, you write yourself malware. What do you want  
20 to do? You want to infect as many devices as possible,  
21 is it not?

22 Of course, you hit the biggest market. So, by  
23 definition, Android will attract a lot of such malware,  
24 and the fact that they allow self-sign apps, yes. Like  
25 I said, it is a give away. I open the door, I open so

1           that anybody can submit an app, including the bad guys,  
2           with a policy.

3       Q. You see that for 2019, the Android devices are 50 times  
4           more likely to be infected than Apple iPhones?

5       A. I mean, look, even if it is 100 times, I am not  
6           surprised. Because like I said, iOS from day one  
7           require, oh, by the way, they require \$99 per year to  
8           register. Okay, that will stop all the school kiddies,  
9           meaning that your high school kids now cannot register  
10          as an app developer for Apple, because 99 bucks from a  
11          credit card.

12                So my point is their bar is so much higher than  
13            Android. Android says, okay, let us open it up so  
14            anybody can be a developer, including the bad guys.  
15            Because why? We do not check. Okay. Like I say,  
16            I would not be surprised to see that the Android market  
17            has a hundred times more malware than iOS, because,  
18            again, that is not due to the technical incompetence of  
19            review, it is the policy of allowing what can be  
20            submitted.

21                Also, hold on, I would have said the App Store has  
22            failed so many times. Even if Android had the same  
23            percentage in terms of technical capabilities, just  
24            because of the sheer volume of malicious apps submitted  
25            to Android, you will see that the Android market, like

1 Play Store, will have many, many more malicious apps  
2 even when Android, the technical review is as good as  
3 Apple.

4 Q. So, as you say, the fact that it might be 50 times or  
5 100 times more infected on Android devices does not  
6 surprise you?

7 A. No.

8 Q. It would not surprise you if the figures were the same  
9 for 2022 or 2023, your answer is the same?

10 A. Hold on, in 2023, the same RiskIQ report said now go to  
11 Android Play Store. Why? I bet that was the effect of,  
12 since 2021, August, they enforced, at least on  
13 Google Play Store, enforced developer identification and  
14 sign apps. So that is why in the RiskIQ report,  
15 page 15, I read it all weekend, they said go to  
16 Google Play Store. To me, what does this say to you?  
17 It essentially confirms my intuition that once you close  
18 the door, you are much better off. RiskIQ recommends  
19 that.

20 Q. Can we look at the RiskIQ -- sorry, did you say RiskIQ  
21 or Nokia?

22 A. I think RiskIQ, 2023, compared with -- you can contrast  
23 that with the 2020 report.

24 Q. Sorry, Dr Lee, there is no RiskIQ report for 2023.

25 A. Well, it may be Nokia. I do not remember. If you allow

1 me, I can go to my report and ...

2 Q. I think, in fairness to you, I think it is the Nokia  
3 report. Shall we go to that, and that might jog your  
4 memory. {D1/1473/12}.

5 So this is -- as you recall, they look at infections  
6 on devices by reference to fixed broadband and then  
7 mobile networks. So on the right-hand side we have  
8 "Infections by device". Do you see that?

9 A. Okay.

10 Q. You see "phone", skipping ahead, "devices using Android  
11 OS are responsible for 30% of malware activity". So  
12 Android 30%. "Malware that is platform independent ...  
13 24%". But the iPhone is not even ranked here.

14 A. Mm-hm.

15 Q. If you go to page 14, {D1/1473/14}, again "Infections by  
16 device", now we are looking at malware on mobile  
17 networks. "Android-based systems ... the most targeted  
18 ... 49% of all infections". Again, no mention of iOS or  
19 Apple. Have you any reason to disagree with these  
20 figures?

21 A. No.

22 Q. Is there anything else you want to show us in this  
23 report?

24 A. Like I said, page 15.

25 Q. Can we go to page {D1/1473/15}.

- 1       A. Yes, so the left column says:
- 2                "Android users can protect themselves ..."
- 3                The last sentence of the column, the left column,
- 4       says:
- 5                "Android users can protect themselves by only
- 6       installing applications from secure app stores like
- 7       Google Play ..."
- 8                So obviously now Google Play is a secure store
- 9       according to this report.
- 10       Q. Well, let us read the rest of that paragraph, Dr Lee:
- 11               "... most smartphone malware is distributed as
- 12       Trojanised applications and since Android users can load
- 13       application from just about anywhere, it is much easier
- 14       to trick them into installing applications that are
- 15       infected with malware."
- 16               Do you agree with that?
- 17       A. I agree with that, I think, because there are other
- 18       markets, although some of the other stores, they still
- 19       do not enforce identification of developers and they
- 20       still do not enforce signed apps, so that is why the
- 21       recommendations go to Google Play, because now
- 22       Google Play essentially follow a policy which is similar
- 23       to iOS.
- 24       Q. Meaning go to Google Play, do not go to a third party
- 25       app store?

1 A. They did not say so, but say, hey, look, you are better  
2 off downloading apps from Google Play.

3 Q. Can we go to the right-hand side of page 15 under the  
4 column, furthest right column, "Trojanized  
5 applications". Do you see that, Dr Lee?

6 A. Can you zoom in there. The colour ... Thank you.

7 Q. "The most common way malware gets into a mobile device  
8 is for the device owner to be tricked into downloading  
9 and installing an app that contains malware. For  
10 Android users specifically, this risk can be somewhat  
11 mitigated by installing applications only from secure  
12 and trusted app stores, such as Google Play, and by  
13 installing anti-virus product ..."

14 So they are saying use Google Play, do not use third  
15 party app stores?

16 A. They do not say so. They say such as.

17 Q. That is obviously what they mean, is it not?

18 A. No, they they say such as eating Apple. Does it mean  
19 you would only eat Apple? No. Apple is one example.

20 Q. No, they are saying use Google Play instead of a third  
21 party app store.

22 A. No, I thought your question is "secure and trusted app  
23 stores". The language here is:

24 "... from secure and trusted app stores, such as  
25 Google Play ..."

1 Q. Yes, but if you are an Android user --

2 A. Hold on, my point is that Google Play, it did not say  
3 Google Play is the only one. That is what I am saying,  
4 "such as".

5 Q. "... such as Google Play ..."

6 A. Okay.

7 Q. Do you accept that they are recommending their users not  
8 to use certain third party app stores on Android?

9 A. So again, I wish this report actually gave us technical  
10 reasons or policy reasons why other play stores are not  
11 as good.

12 Q. Dr Lee, just the question, please. I said you must  
13 accept they are saying: use Google Play or other trusted  
14 stores as opposed to other third party app stores on  
15 Android?

16 A. So, to me, if I am -- I mean, as a tech-savvy person, I  
17 say why, you need to tell me why.

18 Q. It is a different question. We are coming to the why.

19 A. No, my point is this kind of recommendation to a lot of  
20 people is pointless. It is hard to follow. Say, hey,  
21 go there, not there. Do you not ask why?

22 Q. Let us look at something on the why in the National  
23 Cyber Security Centre report 2022. {D1/1273/1}. As you  
24 can see, Dr Lee, this is a part of, the very top of  
25 page 1, it is part of GCHQ, which is the

1 United Kingdom's intelligence and cyber agency.

2 Could you be taken, please, to page 3. {D1/1273/3}.

3 The second column tells you the scope of the study. On  
4 the right-hand side at the very end, do you see it is  
5 "limited to technical security threats ... not  
6 address[ing] privacy ... concerns or the misuse of data  
7 by legitimate actors". Do you see that?

8 A. Yes.

9 Q. Could you go to page {D1/1273/4}, please. First, do you  
10 see the key statistics for UK adults and the degree to  
11 which they are spending time on apps and downloading  
12 them, do you see those numbers?

13 A. Mm-hm, yes.

14 Q. Have you any reason to disagree with those figures?

15 A. No.

16 THE CHAIRMAN: Do you have a date for this, Mr Kennelly?

17 I know we have seen it before.

18 MR KENNELLY: 2022, sir.

19 THE CHAIRMAN: 2022.

20 MR KENNELLY: Just pausing there and looking at those  
21 figures, would you accept, Dr Lee, that in terms of  
22 those statistics for UK adults relating to the use of  
23 apps, that is very different from what we see with Mac  
24 app usage: 87% owning a smartphone, 16% downloading  
25 weekly, nearly three hours a day spent just using apps.

1       A. So for the ownership of phones and how many hours you  
2       spend playing with apps on the phone, those numbers are  
3       pretty agreeable. I myself probably can be one of  
4       those. But downloading apps weekly, I am not sure.  
5       I mean, I used Mac since early 2000. I probably  
6       downloaded more apps to my Mac than on smart phones. So  
7       I do not know, but, like I said, if that is how they  
8       surveyed, okay, I take the numbers.

9       Q. On the far right, Dr Lee, on that page, do see "What is  
10      the risk?"

11             Can you zoom in on that, please, for Dr Lee.

12             So first of all it deals with the harm:

13             "If popular apps ... are compromised, millions of  
14      users are potentially vulnerable ..."

15             Do you see that?

16      A. Yes.

17      Q. Then:

18             "... even official app stores (such as Apple ... and  
19      Google's Play Store) with vetting processes ... have  
20      been impacted by malware."

21             But then this:

22             "Furthermore, the current well-known third party app  
23      stores (that is, stores which are not provided by the  
24      manufacturer or the operating system provider) appear to  
25      have less robust vetting processes and so represent

1 a greater risk."

2 Do you agree with that?

3 A. That is what it says. To me, as a technical person,  
4 I normally challenge this kind of statement. What does  
5 it mean by "appears"? That means, hey, can you show me  
6 what kind of analysis you have used to draw this kind of  
7 statement. Do you actually compare the technical review  
8 process of third party app store versus Google Play or  
9 Apple, or you just, okay, numbers in this, and conclude  
10 it must be the technical review. Like I said, there are  
11 other factors, such as these other stores insist on  
12 identification, verification and app signing. To me, it  
13 is not rigorous.

14 Q. So you think that the conclusion here from the National  
15 Cyber Security Centre, from GCHQ, is not rigorous?

16 A. I am saying just when you show this statement to me and  
17 say do you agree or not, that is not enough data points.  
18 I need to look at their process.

19 Q. Can we move on, please, to page {D1/1273/6}, and it is  
20 "Overview of app stores", and the heading "Third party  
21 app stores".

22 A. I am not seeing that.

23 Q. It is the -- sorry, right-hand side. There we go.

24 A. Yes.

25 Q. "Unlike iOS, the Android platform allows for third party

1 app stores ... These are app stores, users must download  
2 or access separately ..."

3 Then this, Dr Lee:

4 "... typically characterised by their focus on user  
5 and developer freedom (as opposed to the safety and  
6 privacy of users)."

7 As a general statement, do you agree with the  
8 National Cyber Security Centre there?

9 A. If freedom means you do not have to say who you are,  
10 nobody can verify your ID, you do not sign your app,  
11 yes, I agree with that statement. Freedom is actually,  
12 I do not know, I mean, I am not a political scientist,  
13 yes, freedom's great, but you also give the freedom to  
14 attackers.

15 Q. You do not accept that that freedom might be the freedom  
16 to install a wider range of apps?

17 A. Well, the same as developer freedom.

18 Q. Developer freedom?

19 A. Yes. That means any developer can submit any apps, as  
20 opposed to let us say iOS, they insist you pay \$99  
21 effectively for a week to make sure the credit card is  
22 not stolen, and so on. The point is that iOS, you can  
23 say is less free, but actually, you know, the developer  
24 identification, verification and signing apps is a kind  
25 of gate to keep the would-be malicious developers out,

1           whereas some of these other third party stores, as you  
2           know, it is Google policy to say anybody can submit. To  
3           me, that is why we have such a security consequence.

4       Q. But Dr Lee, could this developer freedom not also mean  
5           that the app stores -- these app marketplaces are  
6           applying less robust vetting processes on the apps  
7           themselves?

8       A. Again, like I said, unless this report, the process that  
9           led to this report had a rigorous analysis of that,  
10          otherwise I just cannot agree or disagree with anything  
11          that they say about what are the causes.

12      Q. Let us look at the third paragraph on this column:

13                 "While there's less [or fewer] people using the most  
14                 common third party app stores (compared with official  
15                 app stores) a lack of robust vetting processes means  
16                 that their users are especially vulnerable to threat  
17                 actors uploading malware ... The threats from official  
18                 or third party [app] stores include spyware, banking  
19                 malware, and malware used for toll fraud."

20                 Do you see that?

21      A. Yes, I see that statement, but --

22      Q. Do you disagree again with the National Cyber Security  
23          Centre here?

24      A. So, again, I do not want to disagree with a national  
25          centre for cybersecurity. Obviously they are very well

1           respected, no doubt. The point is you have not given me  
2           enough time or context to read the report and say, hey,  
3           what process did they use to say that it is less  
4           rigorous when they vet? What do they mean by vetting?  
5           Do they mean the static and dynamic analysis of apps  
6           versus vetting the developer's identification? I mean  
7           all that. So, to me, you cannot force me to agree or  
8           disagree without a context.

9           Q. Can we just then, now that you have seen all this  
10           material, go back to your reports and take up {C2/5/14}.

11          A. Can you remind me which report is this?

12          Q. This is your first report.

13          A. Okay, page 14. Yes, thank you. Okay.

14          Q. Paragraph 19.

15          A. Did you say 14?

16          Q. Page 14. {C2/5/14}.

17          A. So this is my first report?

18          Q. Yes.

19          A. Pages?

20          Q. Page 14, paragraph 19.

21          A. Paragraph 19, okay.

22          Q. Halfway down that paragraph, you say:

23                 "... in my opinion third-party app stores can (and  
24                 do) perform security reviews for apps they distribute  
25                 comparably with those used by the App Store, because the

1 standards and techniques employed by all app stores ...  
2 are known and can be replicated consistently."

3 A. Yes, that is what I said, yes.

4 Q. Do you stand by that evidence?

5 A. Yes, absolutely.

6 Q. But "all app stores" including all third party app  
7 stores, Dr Lee?

8 A. Yes, technically they can do it. I stand by it.

9 Q. But it is not that they can do it, they are doing it.

10 Third party app stores can and do perform security  
11 reviews. You are not suggesting that all third party  
12 app stores currently perform security reviews that are  
13 comparable to Apple's App Store?

14 A. So, again, there is no report to say that they are not  
15 doing it either. So, to me, it is like yes, they can  
16 technically, and I believe they do.

17 Q. That is just not plausible in view of what we have seen  
18 in terms of the warnings we have been given by  
19 the government about third party app stores.

20 A. Again, the government report you cited did not describe  
21 the process that they used to draw a conclusion. For  
22 example, what does it mean by vetting? Did they look at  
23 all the technical methods that were used by a third  
24 party store and compare that, let us say, with iOS or  
25 let us compare it with Google? Vetting can also mean

1 different things. It can mean vetting the developer's  
2 history, reputation, verification, all that.

3 So, yes, I do not have reason to believe that third  
4 party stores do not do it.

5 THE CHAIRMAN: Dr Lee, just to be clear here, we are talking  
6 about the security reviews, and this is the equivalent  
7 of the App Review, is it not?

8 A. Yes.

9 THE CHAIRMAN: Is it your evidence that all third party app  
10 stores perform an App Review of that sort, is that your  
11 evidence, or do you not know?

12 A. So I mean -- so, again, let me take a step back, right?

13 THE CHAIRMAN: Just before you do that, I appreciate you are  
14 saying they can do it, but what Mr Kennelly is asking  
15 you is whether you are saying that they all do it. That  
16 is the question.

17 A. Okay, great question.

18 THE CHAIRMAN: So yes or no.

19 A. Great question. My statement did not say "all".

20 THE CHAIRMAN: So that is the question that Mr Kennelly is  
21 asking you, and I just want to be clear whether you are  
22 saying they can do it or they actually do do it. That  
23 is the question.

24 A. Okay, I appreciate that question, right. But my  
25 statement says third party app stores can and do.

1 I did not say "all". So my point is that I am not  
2 excluding the possibility that some app stores is not  
3 doing it, but that, you know, that does not conflict  
4 with my statement here.

5 MR KENNELLY: Page {C2/5/72} of this same report,  
6 paragraph 120.

7 A. Okay.

8 Q. It is the second sentence. You say, in very clear terms  
9 actually:

10 "Apps distributed by third party app stores do not  
11 inherently pose more security risks than apps  
12 distributed by the App Store."

13 That is a statement in the present tense, is it not?  
14 Do you stand by that evidence?

15 A. Yes, that is in the context of iOS, that is why I say  
16 "App Store", with capitalised A and S. That means we  
17 are talking about it in the context of iOS. Nothing to  
18 do with Android.

19 Q. Well ...

20 A. I stand by it, yes.

21 Q. First of all, paragraph 120 begins:

22 "The security, privacy, and safety issues that  
23 Notarization [that is obviously iOS EU notarisation]  
24 aims to identify ... are already present in apps  
25 reviewed and distributed by the [Apple] App Store

1           because just like any app store, the App Store can also  
2           fail."

3           You are making the point that the App Store is not  
4           infallible, right?

5           A. Yes, I am pointing out there is limitation. There is no  
6           such thing as perfect security.

7           Q. Then you say:

8           "Therefore [which we understand to mean following  
9           from your previous point] apps distributed by third  
10          party app store do not inherently pose more security  
11          risks than apps distributed by the App Store."

12          Do you wish to change any part of this evidence,  
13          Dr Lee?

14          A. No. I mean, in the context of my whole report, I talked  
15          about that third party app stores, they have technical  
16          capabilities to do what Apple is doing, Apple's App  
17          Store, and to the extent that sometimes app stores fail,  
18          yes, I expect that sometimes a third party app store  
19          fails, so I stand by this statement.

20          Q. At page {C2/5/87}, please, just focusing on the  
21          chairman's question about App Review. Paragraph 158.

22          Halfway down, you say:

23          "As discussed throughout this report ..."

24          Do you see that?

25          A. Mm-hm.

1 Q. "... third party app stores already provide comparable  
2 app reviews to the App Store (that is, they can meet  
3 these requirements) and will have their own incentives  
4 to do so, if permitted, on iOS (to attract and maintain  
5 as many developers and users ...)."

6 Do you see that?

7 A. Yes.

8 Q. Are you saying that all third party app stores already  
9 provide comparable App Review to the App Store?

10 A. First of all, I did not say "all".

11 Q. You did not qualify it, though, did you, Dr Lee?

12 A. What?

13 Q. You did not say "some" or "the best ones"?

14 A. I just said in general, I did not say "all".

15 Q. So you meant in general?

16 A. I am not excluding any possibility that there will be  
17 one app store that will not meet the requirements. Like  
18 I said, I completely do not believe absolute security in  
19 any way. So, I mean, if I say "all", that means all.  
20 If I do not say "all", I am not saying all.

21 Q. So what you meant to say was "in general"?

22 A. I just say, basically, like I said, throughout my  
23 report, technically any app store can do it now. The  
24 possibility that one app store did not do it, possible.  
25 Maybe sometimes they do not do it. Again, all these

1 things I do not want to exclude, right? But like I say,  
2 in principle, technically my understanding, I stand by  
3 it, is that all technical -- well, any app store, if  
4 they want it they can do it.

5 Q. So let us move on to the causes of these different  
6 outcomes on iOS and what inferences we can draw about  
7 the causes for why there is such a higher rate of  
8 infection on Android devices.

9 A. Okay.

10 Q. We should identify first, would you agree, the key  
11 differences between the security strategies deployed by  
12 each of these different platforms?

13 A. Can you repeat that question again, sorry?

14 Q. Let us look at the differences --

15 A. Okay.

16 Q. -- and I will check if you agree with them. The first  
17 is the one you mentioned, the policy on code signing.

18 A. I just start with developer identification,  
19 verification.

20 Q. Yes.

21 A. Then code signing with a certificate issue by a trusted  
22 party.

23 Q. So I want to put -- so identification and code signing  
24 are different?

25 A. Different.

1 Q. But collectively we will look at them together, but  
2 I appreciate they are different.

3 The second difference is the number of manufacturers  
4 of devices on which the operating system is installed?

5 A. Yes, that is one of the main differences, yes.

6 Q. The third is the distribution and App Review policy of  
7 the platform?

8 A. Yes, that is one of the differences, yes.

9 Q. The fourth is the fact that iOS does not conduct  
10 on-device malware scanning after apps have been  
11 installed. Those are the main differences?

12 A. Yes, not to a degree of, let us say, MacaOS, Microsoft  
13 Windows and Android, in terms of malware scanning, but  
14 there are other security mechanisms that are used that  
15 are common as well. Okay, in general I agree with what  
16 you said, yes.

17 Q. So I think we can exclude malware scanning first,  
18 because if we are thinking about the potential causes of  
19 the disparity and outcomes that we saw on the data, the  
20 presence of on-wear -- on-device malware scanning is  
21 probably not the cause, right, why ... If iOS devices  
22 have such a better record of rates of infection, it is  
23 unlikely to be caused by their lack of on-device malware  
24 scanning?

25 A. Can you repeat the question again, sorry?

1 Q. The absence of on-device malware scanning on iOS devices  
2 is unlikely to be the cause of the differences in rates  
3 of infection that we saw in the data?

4 A. Yes, I think you are right, yes.

5 Q. So we will look at code signing and look at your report,  
6 {C2/5/26}.

7 A. So that is my second report.

8 Q. This is your first report, paragraph 33.

9 A. I am sorry, which page again?

10 Q. Page 26.

11 A. Okay, thank you.

12 Q. In paragraph 33, you describe what is meant by this  
13 policy of identification and code signing, and you say  
14 that for iOS, Apple issues a signing certificate, so the  
15 digital document that specifies the expiration date of  
16 the key that is used for code signing and the holder of  
17 the key, the developer, and by issuing an iOS app  
18 developer with a certificate, Apple has created a valid  
19 key but also verified the identity of the developer.

20 A. Mm-hm.

21 Q. The key is used to sign the apps. So whenever the  
22 operating system runs the app, it verifies that the app  
23 has been signed by the Apple-issued certificate. That  
24 guarantees the key is valid and should be trusted,  
25 because it is from Apple, but also that the developer's

1 identity has been verified.

2 Yes?

3 A. Yes.

4 Q. Now, putting identification to one side and focusing  
5 only on code signing, code signing in this sense does  
6 not involve reviewing the content of the app, does it?

7 A. So, I mean, I do not recall where I said in my report,  
8 right? So code signing actually in Apple is pretty  
9 nuanced. First of all, like I said, you get your ID  
10 verified by Apple. Apple issue a signing key. Then  
11 when you submit an app for review, you just sign using  
12 the key. So Apple knows, okay, that is a developer I  
13 have already verified. Then Apple reviews the app, then  
14 Apple signs using Apple's own key.

15 So, basically, the nuance here, meaning that the act  
16 of signing the app in Apple means that if I check, if  
17 I check, okay, this app has been signed properly, then  
18 I will also know that this app has been reviewed by the  
19 App Store.

20 Q. So there are two different stages I think you are  
21 saying. First, there is code signing in the sense you  
22 describe here, where the developer has his identity  
23 verified by Apple and then he is issued with the key  
24 that he uses to submit the app for review?

25 A. Correct.

1 Q. After App Review, Apple signs the approved app with its  
2 key?

3 A. Yes.

4 Q. But looking -- which only happens if the app has  
5 actually been passed by App Review?

6 A. Absolutely, yes.

7 Q. So we are looking at the prior stage before App Review,  
8 which is just identification and that first stage of  
9 code signing. In that first stage, there is no malware  
10 scan or review of the content of the app?

11 A. You mean at the time they submit?

12 Q. No, pre-submission.

13 A. Pre-submission, yes, okay, sure.

14 Q. The reason why that mandatory code signing at the  
15 beginning is a security tool is because it acts as  
16 a kind of deterrent. Attackers know that if they are  
17 caught distributing malware, Apple will know who they  
18 are and can block their developer account?

19 A. Yes, and the reason for iOS is that the only way that  
20 you can sign your own app in a valid way is to use the  
21 key issued by Apple, and Apple would issue -- sorry,  
22 issue a signing key for you specifically. It is only  
23 after they have verified you, right? So basically it  
24 means that you sign the app and Apple accept your  
25 signature. That means Apple knows who you are.

1 Q. Yes, even before App Review?

2 A. Yes.

3 Q. But even where apps have been submitted to Apple for App  
4 Review, on many occasions those apps were found to  
5 contain malware, were they not?

6 A. Sometimes, yes.

7 Q. Let us look at what Mr Schiller said about sometimes.  
8 {B2/3/30}. It is paragraph 1 -- sorry, it must be  
9 further, paragraph 112 {B2/3/35}. I am sorry,  
10 {B2/5/30}. There we go.

11 This is the first witness statement of Mr -- sorry,  
12 it is Schiller, Mr Schiller. You see paragraph 112,  
13 that even after the developer had been identified and  
14 the key had been issued to the developer, and the app  
15 was submitted for App Review, Apple rejected nearly  
16 1.7 million apps.

17 A. Mm-hm.

18 Q. If you go to paragraph 116 of this document, page  
19 {B2/5/32}.

20 A. Hold on, before you go there, the next paragraph  
21 explains the common causes of rejection.

22 Q. Yes.

23 A. Paragraph 113. So if you go there, I mean, I do not see  
24 security as a main reason.

25 Q. Let us go back to -- to that paragraph 112 again --

1 A. Okay.

2 Q. -- Dr Lee, since you drew our attention to it. Sorry,

3 113 was the one you --

4 A. Yes. So where do we --

5 Q. These are other common reasons for rejections of apps,

6 yes? Is this the one you wanted to see?

7 A. Yes. So my point is that between paragraph 112 and 113,

8 I do not see the main reason as security violation,

9 unless I missed something obvious.

10 Q. Paragraph 116, please. {B2/5/32}

11 A. Okay.

12 Q. So this tells you the breakdown in a fraud prevention

13 analysis. You see at (a), 29,000 apps had hidden or

14 undocumented features; 153,000 spam, misleading users.

15 400,000 privacy violations and at the bottom, 428

16 fraudulent developer accounts were terminated. Do you

17 see that?

18 A. Okay, yes.

19 Q. So all of these apps and fraudulent developers had

20 passed the code signing stage?

21 A. Mm-hm.

22 Q. They had had their identities verified and they still

23 went and submitted these fraudulent or misleading or

24 risky apps to Apple?

25 A. Yes. So, I mean, look, my response is the following:

1           this is a great idea to verify ID even though it is not  
2           perfect. That is still the best we have. Just like  
3           have you not heard of fake driving licence? I mean, you  
4           have teenage kids, that is what they use to get a drink.  
5           Have you not heard of fake passports? Of course you  
6           have heard. So what do they do? Bad idea, do not use  
7           it? Come on.

8           To me, this is the best thing we have, and security  
9           have verified the developer's identification and then  
10          issue a signing key. If they fake it, okay, at least in  
11          security the main way we deal with attack is so-called  
12          raise the bar, meaning that the attacker has to do  
13          something more in order to bypass our checks.

14         Q. But you must see that these figures suggest that even if  
15          it is a deterrent, identification and mandatory code  
16          signing, it is a rather weak deterrent, is it not?

17         A. I do not know. They did not say how many accounts. How  
18          many accounts did they say, and how many years, right?

19         Q. Well ...

20         A. What is the percentage?

21         Q. He said this is what happened in 2022. This is what  
22          they did in one year.

23         A. Okay, but how many accounts?

24         Q. I am sure you can be taken to those figures later, but  
25          in terms of the driving licence example you give,

1 Dr Lee, one of the problems that even Apple has is that  
2 bad actors horde false signing identities so the  
3 identification stage can be -- Apple can be tricked at  
4 that stage by the fact that malicious actors horde false  
5 signing identities?

6 A. I absolutely agree with what you said. But on the other  
7 hand, in reality even though I know that somebody has  
8 fake IDs, fake passport I still want our authority to  
9 check driver's licence and passport so at least they  
10 have a higher bar to guard against criminals. So that  
11 is why yes, you know, some people can bypass Apple's  
12 checks but compared with Android who just does not  
13 check. Which is better? Of course iOS is much better.  
14 It is self-intuitive.

15 Q. I think we can agree, Dr Lee, that it is a contributing  
16 factor, mandatory code signing and identification?

17 A. I will tell you that this is such a huge contributing  
18 factor. I have been analysing malware for 20 years. At  
19 one point I had a Department for Homeland Security  
20 contract which requires us to analyse half a million  
21 malware samples per day. I have not seen malware  
22 samples that declare, I am the author, I am Wenke Lee.

23 Malware author never declare who they are. That  
24 is -- just by intuition. Which criminal want to  
25 declare, I am a bank robber, I am Wenke Lee.

1           But for iOS and Android you have to have  
2           a developer's ID, right. You have to have a developer's  
3           ID in order to put your app on the App Store or Play  
4           Store. So you force them to do something, so that is  
5           iOS say I am going to force to verify you first and then  
6           the attacker tries to bypass that.

7           But my point is if you do not have any checks then  
8           the developers, malicious developer will go back to how  
9           they have been doing in 20, 30 years. Just do not say  
10          who they are.

11         Q. Dr Lee, for all those reasons you still say that  
12           identification and that first stage of code signing is  
13           the most important contributing factor to the security  
14           of iOS devices?

15         A. I stand by it absolutely.

16         Q. Can we go to where you say that. {C2/13/29}, second  
17           report, Dr Lee.

18         A. Okay.

19         Q. I am coming near the end of this topic, sir, and that  
20           might be an appropriate time for a first break.

21         A. Okay.

22         Q. Paragraph 47. Actually, paragraph 46 is where you  
23           mention it as a very significant implication. So in  
24           paragraph 46, please -- can Dr Lee be shown  
25           paragraph 46:

1            "In my opinion" about halfway down the paragraph; do  
2            you see that, Dr Lee?

3            A. Yes.

4            Q. "...developer verification case and code-signing  
5            policies have very significant security implications and  
6            are materially more significant to security on any  
7            platform than App Review and app distribution models."

8            You give a footnote 99; do you see that?

9            A. Mm-hm.

10           Q. Then you say in 47 it is the most important contributing  
11           factor, top of 47?

12           A. Yes.

13           Q. So for such a strong statement we look for support and  
14           you cite at footnote 99 a white paper by Entrust, "The  
15           importance of code signing"; do you see that?

16           A. Yes.

17           Q. Can we go to that, please, {D2/608/4}. Now, just to  
18           understand, Entrust, their business is to provide code  
19           signing services, to generate certificates as  
20           a so-called trusted authority; is that right?

21           A. That is our understanding, yes.

22           Q. So they have an interest in emphasising the importance  
23           of code signing, do they not, a commercial interest?

24           A. Well, okay, but the reason I cited this -- the reason  
25           I reference this report is to explain what code signing

1           really is and how it is being used in the industry, yes.

2           I am not trying to advertise Entrust.

3       Q.   But even Entrust does not say in this document that  
4           developer verification and code signing is more  
5           important than App Review or an app distribution model?

6       A.   But did they talk about App Review or app distribution  
7           at all?

8       Q.   No.

9       A.   So why do they compare? Why do they say, hey, this is  
10          more important than App Review. That is out of context.

11      Q.   Dr Lee, I am looking for some support for your statement  
12          that identification and mandatory App Review is the most  
13          important contributing factor to the security of iOS  
14          devices, and I am looking in vain, because Entrust does  
15          not say, does it?

16      A.   They do not.

17      Q.   In fact --

18      A.   Like I said, well, if you say why I say that, I would  
19          say based on expertise. I have been dealing with  
20          malware for decades. In fact, I do malware analysis.  
21          Just so you know, it is actually more challenging than  
22          any App Review that we can talk about, so ...

23      Q.   But is that not even more striking, Dr Lee, that in your  
24          20 years of extensive expertise in this very area, you  
25          have not been able to locate a single study that says

1           that developer verification and code signing policies  
2           are more important for iOS device security than App  
3           Review or Apple's distribution model?

4       A.   Look, the reason is so simple.  You can ask any malware  
5           analyst.  They will tell you they have not seen  
6           a malware that declares who the author really is.  So  
7           the point is that is not a feature, that you have an  
8           author of the malware.  So that is why we do not talk  
9           about it.  We just assume, which is a fact, that the  
10          malware that you got is authorless.  Not only that,  
11          because it is so challenging, it is always obfuscated.  
12          You talk about bait-and-switch, that is nothing compared  
13          with malware.

14       Q.   All the more reason for people like you, Dr Lee, to  
15           investigate how it can be best stopped and what is the  
16           best reason for Apple's superior security protection.

17       A.   That is why I said code -- you know, developer  
18           identification, verification, code signing is such a big  
19           deal.  Because on the open internet we cannot enforce  
20           it.  Most of the time when we get an attack, we do not  
21           know who wrote the malware, we do not where the malware  
22           was released.  Even a high profile hack, that is Sony  
23           Pictures hack, took NSA many, many months to say we  
24           think it is North Korea.  Okay?

25           So that is why we, working in security for so long,

1 we know you can assume that malware will not tell you  
2 who they are, where they are from. So that is why iOS  
3 policy is so powerful. That is why I say it is more  
4 important than anything you do in App Review. I do  
5 malware analysis which, like I said, is much, much more  
6 challenging than App Review, so trust me.

7 Q. So, Dr Lee, it is true that you have not been able to  
8 identify any study or research any article, not even by  
9 you, Dr Lee, that says that developer verification and  
10 code signing is actually more significant for iOS device  
11 security than App Review or apps distribution model?

12 A. I am not sure, I mean, there may be some of our academic  
13 papers talk about Apple's policy. I am sure we mention  
14 App Review. Now, whether we say that is more important  
15 or not, we may not. Like I said, the only reason is  
16 that that is not something that you expect in open  
17 internet. So people like us, we say, yes, you know, it  
18 is obvious. If you enforce it, how to put it, that is  
19 a sea change compared with open internet. So that is  
20 why iOS is so much more -- you know, seeing so much  
21 fewer malicious apps than Android.

22 MR KENNELLY: That is an appropriate moment for a break?

23 THE CHAIRMAN: We will take a break. Thank you.

24 (11.45 am)

25 (A short break)

1 (11.55 am)

2 THE CHAIRMAN: Mr Kennelly.

3 MR KENNELLY: Thank you, sir.

4 Dr Lee, we are now moving on to the next difference  
5 between Apple's approach and that of Android, and that  
6 is the difference in manufacturer numbers. Can we look  
7 at {C2/13/29}. This is your second report. Actually,  
8 page 28, so you see the beginning of the paragraph,  
9 paragraph 45. {C2/13/28}.

10 You are disagreeing with Professor Rubin about the  
11 reason for security differences or security outcomes  
12 between Android and iOS. You say it is not because of  
13 the centralised distribution model. Then over the page,  
14 and this is the important part, Dr Lee, top of page 29,  
15 there are two contributors that are more important:

16 "... (i) the fact that Android developers are able  
17 to sign their own apps without using certificates issued  
18 by trusted certificate authorities ..."

19 Which we have just discussed.

20 "... and (ii) the existence of multiple  
21 manufacturers of Android devices (rather than a single  
22 vertically integrated device manufacturer and operating  
23 system owner [like] Apple ...)."

24 Then you go on to say in the last sentence:

25 "In terms of materiality, the existence of multiple

1 manufacturers of Android devices is the biggest  
2 contributing factor to the difference in security  
3 between iOS and Android."

4 Do you see that?

5 A. Yes, I see that, yes.

6 Q. So there is a difference, is there not, between the  
7 evidence you gave in your first report and the evidence  
8 you are giving here in your second report, this emphasis  
9 on multiple manufacturers?

10 A. Let me look at the context.

11 Q. Paragraph -- let us go back to your first report,  
12 Dr Lee. It is page 65 of your first report. {C2/5/65}.  
13 Paragraph 107.

14 Paragraph 107 of your first report. You said,  
15 second sentence:

16 "In my opinion, the main cause for this Android  
17 security issue ..."

18 That is, in the first sentence, that Android device  
19 users have downloaded many malicious Android apps from  
20 third party app stores. You say the main cause is that  
21 Android allows apps to be self-signed by developers  
22 rather than using certificates issued by trusted  
23 authorities, and you explain why that is a problem, and  
24 you say that can be avoided by requiring mandatory code  
25 signing.

1           So here, when you were discussing the difference  
2           between the problem that Android experiences and iOS,  
3           you did not mention the existence of multiple  
4           manufacturers as a potential reason at all, but in your  
5           second report you said it was the most important reason?

6       A.   So the way to look at this is -- I mean, I am not an  
7           English major, so my wording, choice of wording may not  
8           be the best, but look at the context, right? So the  
9           first report, we are talking about app distribution and  
10          restriction.

11          So 107, when I mention self-signing, this is  
12          something that iOS, if they open up, they can still  
13          enforce. Whereas in the second report I talk about  
14          different hardware or device manufacturer, that is not  
15          something that iOS can fix. The difference is right  
16          there. So that is why I -- maybe I should not use the  
17          biggest contributing factor, but definitely that is  
18          a very major contributing factor. I mean, a factor --  
19          the sentences preceding this sentence talks about these  
20          are two main factors. One is lack of self-signing, the  
21          other one is multiple manufacturers. One of them, Apple  
22          can do something about it. You know, if you want to do  
23          a comparison. The second one, Apple would not be able  
24          to do anything about it.

25       Q.   But nowhere in the first -- I fully understand you may

1           make textual errors or things can be expressed  
2           differently, but nowhere in the first report do you say  
3           the existence of multiple manufacturers is the main or  
4           even an equally important reason to self-signing by  
5           developers as a reason?

6           A. There is a reason of course. The second report, the  
7           title is "Reply", a reply to Dr Rubin's report. So I --  
8           obviously there was a need to bring up, to discuss all  
9           these factors, particularly in response to his report  
10          when he cites some of those industry reports that I do  
11          not agree with their conclusion or their causal analysis  
12          or lack of. So that is why it prompted me to say, ah,  
13          let me go beyond the very basic, which is the code  
14          signing. Let us go beyond that and, you know, talk  
15          about this other contributing factor as well. That is  
16          the context as I remember it.

17          Q. Certainly; and is not what happened, when you saw  
18          Dr Rubin's reply, you realised that mandatory code  
19          signing was actually a weaker deterrent against malware  
20          than you realised and you thought I had better come up  
21          with something else?

22          A. No, that is not the motivation, no.

23          Q. The reason why you say multiple manufacturers lead to  
24          poor security outcomes is because there is  
25          a fragmentation in the number of people responsible for

1 providing software updates. Can I show you your report  
2 again, Lee 2, paragraph 49. It is on page {C2/13/31}.  
3 If you go over the page -- page 31, please. Below the  
4 italicised text, you say:

5 "The significance of this difference ..."

6 The difference in the fact that there are multiple  
7 manufacturers for Android software or Android devices.

8 "... is that responsibility for Android software  
9 updates is shared between Google, network operators, and  
10 multiple device manufacturers, rather than ... sitting  
11 solely with Apple. There is therefore more  
12 inconsistency in the frequency and timing of updates on  
13 Android devices."

14 Do you see that?

15 A. I see that, yes.

16 Q. Let us look at the degree, Dr Lee, of Android OEM  
17 fragmentation in the UK. Can we look at {D1/1295/33},  
18 please. This will be on your screen, Dr Lee.

19 A. Okay.

20 Q. This is a page from the CMA report discussing market  
21 share of different smartphone manufacturers. 3.16. You  
22 see the Apple market share in the first bullet, and then  
23 this in the second, "between 20-30% of new smartphones  
24 ... [are] Samsung". That is "the largest manufacturer  
25 of Android devices". The second largest manufacturer

1 used to be Huawei at 5 to 10%, but that declined because  
2 it has been prohibited from accessing  
3 a Google-compatible version of the Android operating  
4 system.

5 If we go over the page {D1/1295/34}, there is  
6 a reference to Google's Pixel smartphone, zero to 5% of  
7 new smartphone sales. Figure 3.1 gives us, if you  
8 ignore Apple, the major Android manufacturers. Do you  
9 see that?

10 A. Mm-hm.

11 Q. There obviously are other manufacturers manufacturing  
12 Android-compatible devices, but they are obviously not  
13 significant enough to warrant a mention, are they?

14 A. Yes.

15 Q. So if we think about the UK market at the end of the CMA  
16 survey period, there are really only two manufacturers  
17 producing smart phones, Google and Samsung?

18 A. You mean Samsung and Huawei or Google and Samsung?

19 Q. No, Google and Samsung. Huawei by the end of the period  
20 is too small.

21 A. Okay.

22 Q. But certainly Huawei was there for the claim period, so  
23 we will include Huawei, so three manufacturers.

24 A. Okay.

25 Q. So if we look at the global market shares as well, just

1           because some of the data we are looking at is global as  
2           well as UK, can we have {D1/1882/1}. I am afraid this  
3           is going to be an Excel spreadsheet, because this should  
4           be giving us -- yes. There we have from 2016 to 2023  
5           global market shares, and we see Samsung at the top, do  
6           you see that, Dr Lee?

7           THE CHAIRMAN: Mr Kennelly, what is this document?

8           MR KENNELLY: This is the global mobile device statistics  
9           and I will check where it comes from. Statcounter. It  
10          is one of the entities that provide market data,  
11          publicly available market data.

12          THE CHAIRMAN: So is this something you have -- your team  
13          has accessed and put in here, rather than coming from  
14          the expert?

15          MR KENNELLY: Ms Higgins will tell me where it has come  
16          from, I cannot remember the origin of this document.  
17          Obviously --

18          THE CHAIRMAN: It may be that Dr Lee recognises it. I do  
19          not want to take you out of your way. Just out of  
20          fairness to him, I want to understand --

21          MR KENNELLY: Of course.

22                 Dr Lee, we will check where the document comes from,  
23          but really it is a very basic point I am putting to you,  
24          which is when you look at the market shares globally,  
25          what you see is Samsung at the top with 31%. I am

1 looking at Android manufacturers. Then you have  
2 a couple at the top, just below Apple, with shares  
3 around 6%, 7%, and a long tail of manufacturers of much  
4 smaller market shares.

5 A. Mm-hm.

6 MR KENNELLY: Sorry, it is the data the CMA market study  
7 relied upon.

8 THE CHAIRMAN: I see. So this is global, but they would  
9 extract UK from it.

10 MR KENNELLY: Yes. I think they also -- I cannot warrant as  
11 to every precise use the CMA made of it, but that is  
12 where it comes from.

13 THE CHAIRMAN: Thank you.

14 MR KENNELLY: So Dr Lee, again, really the main Android  
15 manufacturers are concentrated into a relatively small  
16 group, even globally.

17 A. So I am curious, where is Google? Why is Google not on  
18 the list?

19 Q. That is a good ... Row 20, there it is.

20 A. It is different from the chart you showed earlier,  
21 right?

22 Q. Sure. The chart I showed you earlier was UK only.

23 A. Okay. This is global. Interesting.

24 DR BISHOP: (No mic - inaudible).

25 MR KENNELLY: Yes, I had the same question. I am afraid

1           there is no clue in the CMA report that I could find as  
2           to what that means. But the basic point, hopefully,  
3           Dr Bishop and Dr Lee, is we are seeing a relatively  
4           small group of major manufacturers and, again, if, if  
5           software update delays were such a major cause of  
6           infections, would you not expect Samsung to be as  
7           insistent as Apple on ensuring their users updated  
8           software and downloaded security patches? Samsung.

9           A. So I mean, first of all, let me correct myself. When  
10          I say material, the different manufacturers, the biggest  
11          factor, I really meant that this is something that  
12          cannot be changed, even in Android. Whereas sign apps,  
13          yes, maybe overnight or over a period of time, all the  
14          Android Play Store -- all the Android app stores decided  
15          to check developer ID or sign apps, whatever. So that  
16          is a difference that can be fixed.

17                 But in terms of manufacturers, multiple  
18          manufacturers, that materially cannot be changed. So  
19          I am going to stand correct what I just said earlier,  
20          a moment ago. In terms of Samsung, just so you know, I  
21          know plenty of people working there, including my former  
22          students. I have a lot of respect for what they do, so  
23          I would not doubt that they would actually do something  
24          similar to Apple, in terms of updated software, and so  
25          on and so forth.

1           But, on the other hand, these hardware  
2           manufacturers, they have their own version of Android.  
3           So really it means that when they see a need to update  
4           Android, they really need to basically customise that  
5           update to their own version of Android, do a lot of  
6           internal testing, and so on, so there is always inherent  
7           delay. Not that they do not want to do it, they want to  
8           do it, but just because they are a different hardware  
9           manufacturer, different, you know ... So in technical  
10          terms, maybe they have different firmware, whatever, so  
11          it takes more time, there is a delay.

12         Q. But Samsung has a powerful incentive to prevent  
13          infections on its devices, does it not?

14         A. Okay, they do, yes.

15         Q. So you would expect them to be hassling their users to  
16          make the necessary updates and the download patches --

17         A. I would think they do, yes.

18         Q. -- to avoid those infections?

19         A. I would think they do.

20         Q. So if security update delays, if this inconsistency was  
21          such a major cause of infections, you would expect  
22          Samsung to be really pressing them as much as Apple  
23          presses its users?

24         A. I am sure all manufacturers say they try their best,  
25          which they do, but it takes time to write software and

1           it takes time to test your update to make sure they  
2           work. It is not like, hey, do it. I want to see it the  
3           next second. No, you cannot.

4           So my point is the fact that if they have a delay,  
5           it does not mean they are not trying their best or they  
6           are not the best.

7       Q. Similarly, Google. Google is the owner of the Android  
8       operating system. It seems inherently unlikely they  
9       would be lagging behind others in rolling out software  
10      updates?

11     A. But, again, it depends on who discovers the bug or the  
12     need to update first, right? If they discover  
13     internally, then of course they will link up. But if  
14     somebody else put it to them, then they will spend time  
15     to investigate and figure out what is the best fix that  
16     can be put into their version of Android.

17           So my point is it takes time. You just do not  
18           install fixes like, how to put it ... I mean, there is  
19           a notion in software engineering that the more code you  
20           put in, the more bug you have. Sometimes your fix, if  
21           you are not careful, you actually introduce a new bug.  
22           So a fix is not something that you take lightly. You  
23           actually take it very carefully. It takes time.

24     Q. But ultimately, if you are looking at the extent of the  
25     fragmentation between the major Android OEMs, in the UK

1           it is very small, there is only a small number of  
2           relevant Android OEMs, and even globally there is a  
3           seriously concentrated group at the top, so we are  
4           talking again about a small number of main Android OEMs.  
5           So the degree of fragmentation between them is quite  
6           limited, is it not, as in the number of Android OEMs  
7           that really count?

8           A. I am not quite following your logic. My point is that I  
9           think the main side effect of having multiple  
10          manufacturers, however a manufacturer is, they have  
11          their own version of Android, so they have to figure out  
12          their own version of fixes, so they have their own  
13          delay. They are nothing to do with the market share,  
14          that is a job they just have to do. Even if they have  
15          one customer, they still have to do it. When you talk  
16          about market share, why does that matter?

17          Q. So you are saying even for the small number of large  
18          ones, the delays between them in updating software is  
19          the most important reason why we see a much higher rate  
20          of infection on Android devices than on iOS?

21          A. I am talking about materially, that is something that  
22          Android cannot fix, there would be multiple  
23          manufacturers, and the delay is inherent because of  
24          that, and nothing to do with market share.

25          Q. No, please answer my question, Dr Lee. Even for the

1 small number of main manufacturers, are you saying that  
2 the inconsistency between them in terms of software  
3 updates, that that is the main reason why we see such  
4 a big difference between the rate of infection on  
5 Android devices rather than iOS devices; yes or no?

6 A. I would say it is one of the main reasons. I listed two  
7 main reasons. The first one is app signing, the second  
8 one is the fact that there are multiple manufacturers.  
9 As I said earlier, the reason I said materially that is  
10 the biggest factor is that is something they cannot fix.  
11 That is physics, almost. Basically you would have  
12 different manufacturers. Whereas code signing, yes, you  
13 can do a policy change.

14 Q. Dr Lee, you mentioned a second ago that one of the  
15 problems is when one manufacturer sees a problem the  
16 other manufacturers may not be aware of it?

17 A. That is not what I said. What I said is that, yes, they  
18 would be aware because they would be notified, but they  
19 need to internally figure out how do they make their fix  
20 to their own version of the Android. That takes time.

21 Q. Is there no risk that where different manufacturers are  
22 seeing problems at different times, there may be delays  
23 in notifying the other manufacturers of the problem they  
24 have seen?

25 A. So, again, I do not know why people would delay it.

1 Q. Sorry, do you know -- what did you say? Ah yes, you do  
2 not know why they would delay it.

3 A. I do not know why they would delay. What is the  
4 motivation?

5 Q. But you do not know the extent to which they do delay,  
6 if they do?

7 A. Look, these people know each other. I would expect they  
8 work with each other, right? So let us say you delay so  
9 that embarrasses you. Next time, you embarrass me.  
10 What is the point?

11 Q. Let us look at the extent to which you actually have any  
12 studies or research to back up what you are saying.

13 A. I am using common sense.

14 Q. Page 38, please, second report, paragraph 67.  
15 {C2/13/38}.

16 A. Okay.

17 Q. It is paragraph 67, and you note at the bottom of  
18 paragraph 67 that other reports have acknowledged that  
19 different OEMs roll out Android security patches at  
20 different times which makes the devices more vulnerable.  
21 Do you see that?

22 A. Yes.

23 Q. Then you say:

24 "I am not aware of any report (including the Nokia  
25 report) that provides a breakdown of the statistics or

1           any analysis to show the real impact of uneven security  
2           updates."

3           Do you see that?

4           A. Mm-hm.

5           Q. So you are not aware of any report that provides any  
6           data or analysis to show the real impact of uneven  
7           security updates between Android manufacturers?

8           A. Okay. So, again, for my proper limited search I did not  
9           find an industry report on the real impact. Now that  
10          you talk about it, I do recall an academic paper which  
11          talks about at least how uneven, the updates get rolled  
12          up. I think they also mention because of that some  
13          attacks will still succeed on devices who actually have  
14          delayed update.

15          I am sure -- I am sure this paper was published by  
16          authors from Indiana University, I do not remember  
17          exactly when. So now I stand corrected that I do recall  
18          now an academic paper. But in terms of industry report,  
19          maybe -- from my limited search I have not found one  
20          that talks about the impact.

21          Q. You have not tried to assess the speed with which  
22          Android OEMs roll out updates?

23          A. I have not studied the speed or measured it, but like  
24          I said, it is a very commonly understood and accepted  
25          fact among the -- within the research -- security

1 research community that this is a problem.

2 Q. You do not assess the security impact of any differences  
3 in the speed with which OEMs roll out updates?

4 A. So impact is harder in general. I mean, you have -- do  
5 you -- I do not know, it is a major undertaking, let us  
6 put it this way. You have to take all the recent  
7 attacks to see what platform fixed their device to  
8 mitigate those threats at what time. It is a major  
9 undertaking, so I do not think I see a lot of people  
10 doing it yet.

11 But like I said, this is a very well understood  
12 fact, and the impacts basically, like I said, for  
13 security, you do not have to see the actual attack to  
14 see the possible consequence. Some of them are so  
15 obvious.

16 Q. But apart from telling us that it is well understood --

17 A. Also obvious.

18 Q. You just take it on trust that it is obvious?

19 A. No.

20 Q. Because there is no evidence to support what you are  
21 saying.

22 A. We have seen enough attacks. We know the consequence of  
23 patch software, including some of the major  
24 well-publicised ones, like Equifax. Why did they get  
25 hacked? They failed to fix a zero day attack that the

1 patch was there. They just failed to apply it.

2 Q. Dr Lee, you are missing the point. It is not just that  
3 it is a factor, there is no dispute that it is a factor  
4 and it is an important factor for security, but you say  
5 it is the most important factor. Now you say that is  
6 more important, that the existence of different OEMs,  
7 and these delays in updates, is a much more important  
8 reason for the differences in Android and iOS outcomes  
9 than App Review?

10 A. No, okay, like I said, I stand corrected to say the  
11 biggest one. But I say materially. What I meant is  
12 that this is not something you can fix. That is  
13 materially -- that is a fact. You cannot say tomorrow,  
14 sorry, guys, only Google can have the Android devices.  
15 That is not going to happen. On the other hand, for  
16 self-signing -- sorry, for code signing, verifying  
17 developer's identification, I could imagine one day all  
18 the app stores, okay, let us do this. There is a policy  
19 change. So that is what I meant by materially this is  
20 biggest factor, because you cannot change it.

21 Now, in terms of knowing the consequence, and like  
22 I said, this is obvious, we know the consequence of  
23 unpatched software. You do not want to say, oh, let us  
24 see how bad it is. Come on, we have seen plenty of  
25 examples already.

1 THE CHAIRMAN: Mr Kennelly, I think the positions are pretty  
2 clear. I would encourage you to move on when you are  
3 ready.

4 MR KENNELLY: I am coming to the end of this.

5 So just stepping back, you say the fragmentation of  
6 responsibility, the consequence of allowing different  
7 people to manufacture the device causes a security  
8 problem?

9 A. Yes, for security update, yes.

10 Q. But is there not also fragmentation of responsibility  
11 when different people can operate app marketplaces on an  
12 operating system?

13 A. I kind of see what you are getting at, but I would  
14 prefer you to refer me the report where we discuss these  
15 kind of things.

16 Q. Doctor, you are the expert. Is there not also  
17 fragmentation of responsibility when different people  
18 can operate app marketplaces on an operating system,  
19 different people are responsible for the security of the  
20 apps on the marketplace?

21 A. Okay, so if you want to talk about app stores and App  
22 Review, let me reiterate the opinions I have offered  
23 throughout my multiple reports. First of all,  
24 technically, app stores can do the same thing as App  
25 Review. Second of all, in terms of policy, it is much

1 easier to agree upon a policy and adopt that. That is  
2 very different from how a manufacturer just cannot take  
3 their factory away.

4 Q. I am only asking you about fragmentation of  
5 responsibility. Only that. Do you accept that there is  
6 fragmentation of responsibility when different people  
7 are responsible for different security on app  
8 marketplaces?

9 A. Okay, so in an app market, like I said, I do not agree  
10 with the notion of fragmentation, the way you -- the way  
11 they describe it, because technically they can do the  
12 same thing. So there is no fragmentation in terms of  
13 their technical capabilities.

14 Q. But you are relying on different people to do it. That  
15 is fragmentation, is it not? Different entities?

16 A. So how do you define fragmentation, let me ask you that.

17 Q. Different companies.

18 A. Okay.

19 Q. The manufacturer, the operating system provider in iOS,  
20 and then the app stores themselves, the third party app  
21 marketplaces?

22 A. Okay, so let me ask you, is a different supermarket  
23 a different standard in their food? Come on. So my  
24 point, it is a well understood process with well  
25 understood technical approaches, as I said throughout my

1 reports.

2 Q. So you do not accept that this fragmentation  
3 responsibility is equally likely to cause a security  
4 problem as the fragmentation responsibility we see  
5 between the OEMs?

6 A. What I am saying is in terms of app stores and app  
7 reviews, I do not believe, from a technical approach  
8 point of view, there is fragmentation. Like I said,  
9 they can do the same thing and they will.

10 Q. So the main reason, Dr Lee, the main reason in fact, in  
11 view of what we have seen, why we see poor security  
12 outcomes on Android, is more likely to be the fact that  
13 Android does not have Apple's centralised system of App  
14 Review --

15 A. I do not agree with that, I completely do not agree with  
16 that.

17 Q. Let us look at the counterfactual then, Dr Lee, and the  
18 extent to which, just to test the point you just made,  
19 the extent to which centralised distribution is  
20 necessary to secure Apple's current levels of safety,  
21 security and privacy. Let us look at what you say about  
22 that in your first report. {C2/5/57}. I am looking at  
23 paragraph 92.

24 Before we read it, Dr Lee, when I talk about the  
25 counterfactual, we are talking about a world without

1 Apple's distribution restrictions.

2 A. Okay, are you talking about present time?

3 Q. No, this is what would be the case.

4 A. What would, okay. Yes, thank you.

5 Q. Or what would have been the case during the claim  
6 period.

7 A. But that is different, right, what would have been  
8 versus what would be in the future? I am a bit  
9 confused. Like I said, I am not a lawyer.

10 Q. Let us look at them as we go through the report.

11 A. Okay.

12 Q. C2, page 57 you say, paragraph 92, last sentence:

13 "Developers [we have seen this before] and consumers  
14 offer digital content on other operating systems enjoy  
15 comparable (and, at times, additional) security benefits  
16 without requiring a centralised app distribution  
17 model ..."

18 Then, I am so sorry, just to make sure we know what  
19 we are talking about, at the very top of paragraph 92,  
20 Dr Lee, you say:

21 "In [your] opinion, Apple's restrictions are not  
22 required to ensure [either] the safety, [or the] privacy  
23 [or the] security of iOS devices ..."

24 You are covering safety, privacy and security there,  
25 are you not?

1 A. That is what I said, yes.

2 Q. If you go, please, to your second report, page 16, that  
3 is {C2/13/16}. Sorry, we are supposed to be looking at  
4 paragraph 11. So I have given you the wrong reference.  
5 {C2/13/5}.

6 A. Okay.

7 Q. I am so sorry, Dr Lee, I was on the right page. Page  
8 {C2/13/16}, paragraph 31. It is just the last sentence.  
9 Just to make sure we understand how far you have gone in  
10 this report.

11 Last sentence:  
12 "In my opinion ..."  
13 Do you see that?

14 A. Let me see here. Did you say paragraph 31?

15 Q. Yes.

16 A. I can see:  
17 "As I explained ..."

18 Q. No, it is the very last sentence.

19 A. Okay.

20 Q. "... in my opinion, alternative app stores/developers  
21 ..."

22 Yes?

23 A. Okay.

24 Q. "... using direct distribution provide the same standard  
25 of App Review, including human review, as the App Store

1 in the actual world, and would be able to provide this  
2 same standard in the counterfactual ..."

3 Do you see that?

4 A. Yes, that is what I -- yes.

5 Q. If we go back now, please, to page {C2/13/5},  
6 paragraph 11, under the heading "Counterfactual analysis  
7 for app distribution".

8 Over the page, please, {C2/13/6}, you say absent  
9 Apple's restrictions ...

10 Top of the page -- you are referring here to  
11 Dr Rubin's opinion. He says there would be  
12 a reduction --

13 A. I am sorry, I am a little bit slow in terms of following  
14 you. So we are looking at the top of the page. Is it  
15 the first paragraph?

16 Q. Yes.

17 A. Which sentence?

18 Q. It is the one which begins "In my opinion ..."

19 A. Okay.

20 Q. "In my opinion, there would be no reduction in the  
21 security of iOS devices in the counterfactual, where  
22 [the] restrictions never existed or were removed at the  
23 beginning of the relevant period. My opinion is that,  
24 in the counterfactual where there were alternative  
25 distribution channels ... there would be no material

1 reduction in security on iOS devices ..."

2 Then you give four reasons; do you see that?

3 A. Yes, I see that, yes.

4 Q. So we will begin with mandatory code signing, if that is  
5 okay. It is (c). Do you see (c)?

6 A. Yes, sure, yes.

7 Q. For this, you say Apple could require mandatory code  
8 signing with certificates issued by trusted parties when  
9 allowing third party app distribution?

10 A. Yes.

11 Q. Can we go back, please, to your first report on that  
12 point. Page {C2/5/62} Back of your first report,  
13 paragraph 102. Page 62. Do you see where it says "For  
14 example", about four lines down?

15 A. Mm-hm.

16 Q. We are talking about other third parties providing this  
17 identification and certification service:  
18 "... an app developer or a third party app store can  
19 acquire a certificate from a trusted third party  
20 certificate authority with similar standards to those  
21 applied by Apple ..."

22 Do you see that?

23 A. Yes.

24 Q. You give three examples. Do you see that?

25 A. Yes.

- 1 Q. So just pausing there. As we discussed with Entrust  
2 a moment ago, these companies take payment from  
3 developers in exchange for providing them with  
4 a certificate?
- 5 A. Yes.
- 6 Q. So they are competing against one another for business  
7 from developers?
- 8 A. I suppose so, yes.
- 9 Q. So they are concerned to ensure the best developer  
10 experience and price?
- 11 A. I assume so.
- 12 Q. Does that not create an incentive possibly to lower  
13 standards in order to offer a lower price?
- 14 A. I do not know how you operate a supermarket. I do not  
15 know. You want to sell cheap goods? I do not know.  
16 I am not the best person.
- 17 Q. Let us look at DigiCert, that is {D2/398.1/1}. So this  
18 describes the DigiCert code signing certificate service.  
19 Can we go, please, to page {D2/398.1/2}. It tells you  
20 that the price starts at \$49 a month.
- 21 A. Okay.
- 22 Q. If you go over the page -- sorry, down the page, please.  
23 Sorry, forgive me. Just below \$49 it tells you that for  
24 12 months it is \$588, do you see that?
- 25 A. Yes.

1 Q. Does that sound right in terms of DigiCert's pricing?

2 A. I do not know.

3 Q. Can we go to {D1/1840.1/1}. This is an article from  
4 June 2024 about DigiCert revoking thousands of SSL  
5 certificates, so code signing certificates, over  
6 validation error.

7 A. Mm-hm.

8 Q. Can we skip down, please, to look at the article.

9 First paragraph:

10 "In a move that could cause some serious headaches  
11 for website administrators, DigiCert ... is revoking  
12 thousands of SSL certificates due to a technical error  
13 in the company's domain validation process."

14 Do you see that?

15 A. Yes.

16 Q. Were you aware of this problem at DigiCert before you  
17 filed your reply report in September?

18 A. No, to me it really does not matter. To me, this is  
19 well-known issues in so-called public infrastructure.  
20 Because if you rely on a bunch of certificate  
21 authorities, such as DigiCert, Entrust, to do a good  
22 job, every now and then they make a mistake. So that is  
23 why in the DigiCert example, they just revoke the  
24 certificate. That is actually a very standard  
25 operation: you make an error, you revoke it, and you ask

1 the customer to try again, to go through the now fixed  
2 process. When you revoke it you tell everybody, hey,  
3 that previous signature is no longer valid.

4 In fact, when you check your public -- your  
5 signature, you first check a so-called revocation list  
6 to see whether that certificate has been revoked. So my  
7 point is that the issue that you talk about here is  
8 well-known for decades and there are whole industry  
9 standards and practice to deal with this kind of  
10 imperfection, errors and so on and so forth, so I am not  
11 concerned.

12 Hold on. The last thing is that, look, if Apple is  
13 so worried about other third parties, why can't Apple  
14 just -- you know what, I am the authority. You cannot  
15 distribute your app in a third party marketplace. But  
16 I am the authority. I check the developer's ID, which  
17 is the case now in the EU. I issue you the signing key,  
18 which is the case now in the EU. What is wrong with  
19 that?

20 Q. Your evidence is that these certificates authorities  
21 apply standards similar to those applied by Apple. That  
22 is your evidence?

23 A. I do not have any doubt to that. I do not have any  
24 reason to doubt that is not the case.

25 Q. Let us look at Entrust. {D2/429.1}. It is the second

1 of the three. Can we just go back to page 2, please,  
2 just to see the pricing again. {D2/429.1/2}. Stop at  
3 page {D2/429.1/3}. Look again at code signing and you  
4 see the prices at the top of the page?

5 A. Okay.

6 Q. Any reason to doubt those prices?

7 A. I do not know. I do not pay. I do not have any  
8 business with this kind of thing.

9 Q. {D2/969}, next document. It is a post from the Google  
10 Security Blog. The original is from 27 June 2024. Can  
11 we go to page {D2/969/2}, please.

12 "Sustaining digital certificate security -- Entrust  
13 certificate distrust".

14 Can we go down to the two paragraphs before the end  
15 of page 2:

16 "Over the past several years, publicly disclosed  
17 incident reports highlighted a pattern of concerning  
18 behaviours by Entrust that fall short of the above  
19 expectations, and has eroded confidence in their  
20 competence, reliability, and integrity as  
21 a publicly-trusted CA owner."

22 Were you aware of this before you filed your reply  
23 report in September?

24 A. No, I mean, like I said, this -- to me this kind of  
25 concern is, like I said, have been dealt with and

1 normally dealt with by the industry for a long time.  
2 Think about it, if you are Entrust what you are gaining?  
3 You are actually losing the customers. So Entrust has  
4 no incentive to behave badly. In fact, I do not have  
5 the reference but I did read something about Google was  
6 going after Entrust because of some competitiveness but  
7 you know, it does not matter. To me as I look, let us  
8 say Android decides or Google decides not to trust  
9 Entrust or Apple decides not to do that, they can say,  
10 you know what, guys, do not use them, use somebody else  
11 or use me. No big deal. Technically, you know, this is  
12 not a concern to me.

13 Q. Dr Lee, your expert evidence is that Entrust applies  
14 similar standards to those applied by Apple, Entrust?

15 A. So as far as I know when I filed the report, yes, I am  
16 not aware of this report. I have no reason to doubt  
17 that these certificate authorities would try to do bad  
18 things because they will lose business, right? So to  
19 me, as I do the minutes, yes, DigiCert, NSA, they try to  
20 fix it, but they are working on some of the  
21 certificates.

22 Q. It is not a one-off, Dr Lee. Over the past several  
23 years there is a pattern of concerning behaviour?

24 A. So again, I do not have time to go into the details of  
25 what are those patterns but to me it does not make any

1 sense for Entrust to repeatedly upset a big customer  
2 like Google. I mean, there could be some other reasons.

3 Q. Could you go to page {D2/969/4}, please. Can we zoom in  
4 on the -- just below the halfway point: "Over the past  
5 six years..."

6 A. Okay.

7 Q. So we are talking about incentives, Dr Lee, but this is  
8 what happened:

9 "Over the past six years, we have observed a pattern  
10 of compliance failures, unmet improvement commitments,  
11 and the absence of tangible, measurable progress in  
12 response to publicly disclosed incident reports. When  
13 these factors are considered in aggregate and considered  
14 against the inherent risk each publicly-trusted CA poses  
15 ... it is our opinion that Chrome's continued trust in  
16 Entrust is no longer justified."

17 Do you still maintain that Entrust applies similar  
18 standards to those applied by Apple?

19 A. So like I said, without the knowledge of this report of  
20 course I use it as only one example. But given this  
21 report suppose I believe everything this report says, to  
22 me that is silver lining. This tells you this industry  
23 works. Hey, Entrust if you are not behaving, you are  
24 out. Is that not great? Awesome. I have more  
25 confidence in what is said here.

- 1 Q. Six years of --
- 2 A. Okay.
- 3 Q. -- bad behaviour?
- 4 A. Okay, look, Google could have acted more aggressively if
- 5 it was so bad. They waited for six years. Obviously it
- 6 was not bad enough initially. But the point is it does
- 7 not matter. We are arguing for minute detail here.
- 8 Completely pointless. My point is that this report to
- 9 me is a silver lining. It means this industry works, so
- 10 we should trust having these kind of certificate
- 11 authorities. You know why because they form
- 12 a community, they work together, they exclude bad
- 13 behaviours if the bad behaviours is really behaving
- 14 badly, consistently. Is that not awesome? I wish other
- 15 industries performed that way.
- 16 Q. You say it is a minute detail, your words Dr Lee, but
- 17 obviously for Chrome they considered it an inherent risk
- 18 allowing them to continue for the whole internet
- 19 ecosystem?
- 20 A. So why didn't Google say, get off year one if it was so
- 21 serious?
- 22 Q. It was not a minute detail for the website operators who
- 23 had to get a new certificate from a different authority,
- 24 was it?
- 25 A. So again, if Google knew about Entrust, of this kind of

1           behaviour and this behaviour is bad enough, I am  
2           surprised they do not act more forcefully in year one  
3           instead of waiting for six years. That does not make  
4           any sense to me.

5           Q. Can we go to {D1/1,840.2}. This is an email from  
6           Ben Wilson of Mozilla on 31 July 2024. Mozilla operates  
7           the Firefox web browser, does it not?

8           A. Yes.

9           Q. This is Mozilla's decision to distrust the same website  
10          certificates?

11          A. Okay.

12          Q. Can we look at paragraphs 1-3, please. Can you read  
13          those to yourself, Dr Lee?

14          A. Which paragraph, can you repeat?

15          Q. 1-3, please.

16          A. Okay. (Pause). Okay.

17          Q. Were you aware of this before you filed your reply  
18          report?

19          A. No.

20          Q. Can we go to your reply report, {C2/13/29}. It is  
21          paragraph 47.

22          A. Okay.

23          Q. We actually looked at this earlier. Because you make  
24          the point about third party certificate authorities  
25          having similar standards. Then you cite, if you go to

1 footnote 99, the bottom of the page, you can see it  
2 there, you actually cite a footnote from Entrust's  
3 website?

4 A. Yes.

5 Q. You accessed that on 8 September 2024?

6 A. Yes.

7 Q. So you were on Entrust's website on 8 September 2024  
8 looking for additional material on certification  
9 authorities?

10 A. I was trying to find an article that explain what is  
11 code signing and why it is important. I did not look  
12 into Entrust's relationship with Mozilla and Google, no,  
13 I did not.

14 Q. So you did not notice on the Entrust website the blog  
15 post published by Entrust's president and CEO explaining  
16 how it was going to react to Google's decision to  
17 distrust its certificates?

18 A. So to me, like I said, the point is that awesome, now  
19 they get banned. That means that the industry works.  
20 We should really trust the industry to self correct.  
21 Again, having certificates, having signifying is the  
22 best thing we have in security. I am just that serious.

23 Q. You still maintain they are applying similar standards  
24 to Apple?

25 A. I am saying that by and large we should trust that

1 authority that has business. They must be good enough  
2 that people would trust and use their service and if  
3 they do not consistently they will be banned.

4 Q. But Dr Lee, of the three -- you mentioned three.

5 A. Okay, so let me correct myself. I have been doing this  
6 forever. I am not saying everybody should use Entrust.  
7 I am saying that is one example. Okay. So I mean it is  
8 like, hey, App Store, when they mention the DSC that it  
9 is going to be perfect, no, they are going to make  
10 a mistake too.

11 Q. You only mentioned three and you said in terms these  
12 applied similar standards. So do you accept that  
13 Entrust does not apply similar standards to Apple or did  
14 not before your report?

15 A. Those examples of authority there, no, but like I said,  
16 if they do not the report that you cited is a perfect  
17 example that this industry works by self correct, right.  
18 They self correct. Entrust did not self correct enough  
19 that they get banned. Awesome. That basically agrees  
20 with everything I said.

21 Q. So your evidence is this is good enough for the purposes  
22 of certification on iOS?

23 A. To me that is the best we can have and if iOS or Apple  
24 does not agree or think that the safer way to do it on  
25 their own way, which is what they are doing in the EU,

1           awesome, go for it.

2       Q.   Let us go to the third of your three examples.

3           {D1/88.1/1}. You see that VeriSign -- just to see what

4           has happened to it. You see that VeriSign has sold its

5           authentication business Symantec in 2010?

6       A.   Mm-hm.

7       Q.   Can you go, please, now to {D2/363.1}.

8           We could not find any pricing for code signing

9           services on VeriSign's own website but if you zoom in

10          here and skip down, please, this suggests that VeriSign

11          is offering a year long certificate for \$598. I think

12          if you scroll -- does that sound right to you?

13       A.   Like I said, I mean, I never bought anything like this.

14          I do not know. I have no idea.

15       Q.   {D1/1,745.1}, please. This is from Apple's website,

16          27 March 2024, the date is at the end of the document.

17          You can take it from me that is its date. Can you read

18          the top, please. It tells you that Apple is taking

19          steps to distrust Symantec certificate authorities.

20       A.   Okay.

21       Q.   From 1 August 2018. It is partially distrusting

22          Symantec's CAs. If you look down at the authorities

23          which are affected, look at the bottom half of page 1,

24          you see VeriSign at the bottom there, you see VeriSign

25          Class 1, VeriSign Class 2. Do you see those?

1 A. Mm-hm.

2 Q. Over the page, a whole list of VeriSign certificates  
3 that are being distrusted by Apple. Were you aware of  
4 this distrusting by Apple of VeriSign when you provided  
5 either of your reports?

6 A. No, I do not but, like I said, it is common knowledge  
7 that these certificate authorities would make mistakes  
8 like granting a certificate to some entities that they  
9 failed to verify. Very similar to Apple App's Store  
10 failed to recognise some of the bait and switch malware.  
11 The point is that the industry works in a sense when  
12 they make a mistake they publish that data in the  
13 revocation list and to verify a signature the first  
14 thing you need to do is to check the revocation list.  
15 That is a standard, right.

16 So my point is this industry already account for the  
17 chance they will make a mistake and then they have  
18 a mechanism for them to publicise their mistake and help  
19 people fix them, help them to fix the mistake. That is  
20 there.

21 Q. Do you accept, Dr Lee, that these incidents show the  
22 problem in asking Apple to place part of its security  
23 architecture into the hands of a third party authority?

24 A. Look, I did not have time to look into this but to me,  
25 in my cynical view would be Apple have incentive to say,

1 let's -- don't use VeriSign, use mine, which is fine,  
2 completely fine. That is what they are doing in EU.  
3 That is okay. It is better than not signing, not  
4 verifying.

5 Q. Do you mean that if VeriSign was allowed to compete with  
6 Apple for certification on iOS Apple would have  
7 a competitive advantage?

8 A. Look, I mean, Apple from all I know reading all these  
9 things for this case is that they want everything under  
10 their control. So to me my view is that, yes, I would  
11 not be surprised that they want to kick out everybody  
12 and say, hey, only use my way of issuing you  
13 a certificate. I am not surprised they would do that,  
14 right. But on the other hand, VeriSign is a very  
15 established company. I do not know many entities say,  
16 do not use VeriSign. I just do not know. I just do not  
17 know enough reports like that.

18 Q. But this evidence shows that these three certificate  
19 authorities do not have equivalent standards to Apple?

20 A. So again, like I said, security, certificate authority  
21 they are known to member states just like Apple I think  
22 Mr Federighi was saying that there are people holding  
23 even Apple's own certificate. So even Apple you can  
24 say, hey Apple, you say you are so great, you also make  
25 mistakes. Yes. You can go to Federighi's transcript.

1           Okay. So to me other people say, hey, do not use Apple.  
2           They let bad guys to hold fake IDs. What is the  
3           difference here?

4       Q. So you are saying that these certificate authorities  
5           have had the same amount of problems with certification  
6           as Apple has had with certification and developer  
7           identification?

8       A. Even Apple has made mistakes too when they verified  
9           identification and issue certificates. They all make  
10          similar mistakes.

11      Q. Does not this show that the developer identification  
12          and -- sorry, the process of certification is  
13          problematic of itself? As you say it is common for  
14          mistakes to arise?

15      A. Look, we went through this before the break, right.

16      Q. Dr Lee, am I right or wrong?

17      A. Nothing is perfect in security including certificate,  
18          including App Review. But having, you know, developer  
19          ID and verification, having app signing as mandatory  
20          requirement, that is still way better than not doing it.  
21          The example I gave. Just because you have fake ID or  
22          fake passport, should we not use passport and driver's  
23          licence? It does not make any sense.

24      Q. If it is so imperfect is it not very unlikely that this  
25          is the main reason why Apple's outcomes are better than

- 1           Android's in terms of infections on devices?
- 2           A. Look, it is so imperfect nobody go to VeriSign. Check  
3           the revenue. You think everybody is stupid.
- 4           Q. The next point I wanted to raise with you was the  
5           question of device and run time mechanisms.
- 6           A. Okay.
- 7           Q. Just to touch on this briefly, because you say that  
8           Android has the equivalent of Apple's on device and run  
9           time security mechanisms anyway, do you not?
- 10          A. So throughout my report, you put one report, I described  
11          the on-device hardware security features and also the  
12          operating system security mechanisms. I listed pretty  
13          much comprehensively the list and then my conclusion is  
14          that across the platforms they use very similar on  
15          device security mechanisms and hardware security  
16          features.
- 17          Q. They provide the same security protection, the hardware  
18          and software run time mechanisms, the same security  
19          protection across the platforms?
- 20          A. Yes, some of them provide more.
- 21          Q. Some of them that are on Android?
- 22          A. Android, Microsoft and even Mac OS.
- 23          Q. Provide more than Apple?
- 24          A. Yes, because they are malware scanning.
- 25          Q. Let us look and see what these on-device and software

1 mechanisms can and cannot do. Can we turn to your  
2 report, please, {C2/5/41}. First report.

3 A. Okay.

4 Q. Paragraph 61. Just picking it up on the middle of that  
5 paragraph, it is about half a down that paragraph:

6 "I agree that human review ..."

7 A. Yes.

8 Q. "I agree that human review is a necessary component of  
9 an effective mechanism for protecting user data."

10 A. Yes.

11 Q. So notwithstanding the hardware and software element we  
12 discussed, you still think that human review is  
13 necessary for protecting user data?

14 A. Yes, I mean, I still maintain it is a necessary review  
15 of App Review, yes.

16 Q. Over the page on page {C2/5/42}, paragraph 62 you  
17 mention App Review checking for business model  
18 appropriateness. Beginning of 62:

19 "It screens for unacceptable behaviours including  
20 asking for an unreasonable high price for an app's  
21 features and services ..."

22 Do you see that?

23 A. Yes.

24 Q. That is not something that will be picked up by the  
25 hardware security mechanisms or the software run time

- 1 mechanisms that you described?
- 2 A. Definitely not by hardware but software it really  
3 depends but by and large probably if that kind of  
4 behaviour is being shown to the human reviewers, I would  
5 trust that they can spot it. But maybe in some cases  
6 even the Sandbox would notice that but, again, it  
7 depends.
- 8 Q. Go back to "App Review" and page 33, page 33, please.  
9 Same report. {C2/5/33}, paragraph 46. You mention App  
10 Review. Looking at the second sentence:  
11 "Alongside code signing of apps, I consider this to  
12 be an important security feature."  
13 A. Hold on. Yes, so this I mean App Review, yes.
- 14 Q. For safety, page 39, {C2/5/39}, paragraph 57. You  
15 describe how Apple's App Review checks for objectionable  
16 content. It is paragraph 57.  
17 A. Let me see. (Pause). Okay, yes.
- 18 Q. You accept, do you not, that again, these kinds of  
19 objectionable -- these aspects of objectionable content  
20 would not be picked up by the hardware security  
21 mechanisms or the software run time mechanisms that you  
22 mention?
- 23 A. I did not exclude any sort of -- any of these mechanisms  
24 that you mention because I only talk about the App  
25 Review process. I would say that some of these

1 contents, I think the hardware features may not pick it  
2 up but software you never know. Software, you know,  
3 protection may be able to pick them up.

4 Q. Just to be clear, I was asking you about the things that  
5 the hardware and software run time just could not pick  
6 up?

7 A. Yes, software run time maybe would have picked up some  
8 of these --

9 Q. May do but may not?

10 A. May or may not, right. The same with human reviewers.  
11 They may not spot some of these either.

12 Q. Moving on then to your first reason why there would be  
13 no material reduction for security in the  
14 counterfactual. That third party app marketplace and  
15 developers distributing directly would implement the  
16 same --

17 A. Hold on, where do I see this? Where do I say what you  
18 just said?

19 Q. Do not worry, I am just summarising your first reason.  
20 You said that third party app marketplace and developers  
21 would implement the same standards as Apple. Now I will  
22 show you your first report, {C2/5/59}.

23 A. Okay.

24 Q. It is over the page -- yes, exactly. So it is  
25 paragraph 96, penultimate sentence:

1            "If permitted to operate on iOS, alternative app  
2 stores can and, in my opinion, would provide App Review  
3 as well, which I would expect to incorporate similar  
4 safety, privacy and security checks."

5            Similar to those; I am assuming you mean similar to  
6 those applied by Apple?

7            A. Hang on, I am a little bit slow. Which sentence?

8            Q. It is the second last sentence of paragraph 96.

9            A. You say the second last sentence?

10          Q. Yes:

11                  "If permitted to operate on iOS ..."

12          A. Okay.

13          Q. Do you see that?

14          A. Yes.

15          Q. Is that still your evidence?

16          A. Yes, to the extent that they allow, yes.

17          Q. Then can we go to paragraph 124, page 73. {C2/5/73}.

18                  You say to the extent that they are allowed, but you say  
19                  that actually their incentives will encourage them to  
20                  high standards. Paragraph 124 on page 73.

21          A. Mm-hm.

22          Q. You say:

23                  "There is no reason to doubt that alternative app  
24                  marketplaces would not share the same clear incentive as  
25                  Apple to protect users from safety, security, and

1 privacy threats because the quality of their services  
2 and reputation are key to attracting and retaining  
3 developers and device users."

4 Do you see that?

5 A. Yes.

6 Q. Is that still your evidence?

7 A. I still maintain that opinion, yes.

8 Q. All third party app stores on iOS, if they were allowed,  
9 would have the same incentives as Apple in terms of  
10 safety, security and privacy?

11 A. I say this is a formidable principle, right? I do not  
12 know how you operate business by offering bad stuff. It  
13 does not make any common sense. So I still maintain my  
14 opinion here.

15 Q. One more reference, may I, before -- thank you. So on  
16 the same page, Dr Lee, you explain why you think that  
17 notarisation in the EU is actually unnecessary because  
18 of those incentives.

19 At paragraph 125, you say that what is allowed in  
20 the EU is not a fully open distribution model. All apps  
21 are still checked by Apple first. The only real  
22 difference is that notarisation is a lighter version of  
23 the full App Review. So the third party app stores  
24 potentially require more work. Using them requires more  
25 work for developers because they have to submit their

1 apps for notarisation in the App Store before then  
2 letting third party app stores who may have different  
3 requirements and standards perform their own checks  
4 before the apps can be listed in the alternative  
5 marketplaces. Do you see that?

6 A. Again, I am not following. You said the last paragraph?  
7 Is it paragraph 125?

8 Q. Yes, paragraph 125.

9 A. Okay, and which sentence?

10 Q. Read the whole paragraph to yourself, please.

11 A. Okay. (Pause)

12 Q. Over the page too, where you identify why it is  
13 problematic to let Apple do notarisation, in your  
14 evidence.

15 A. (Pause). Yes, I have finished reading, yes.

16 Q. Paragraph 126.

17 A. 126, too, okay.

18 Q. Just to hurry things along, you say in the second  
19 sentence:

20 "In my view, the app distribution model can be more  
21 open without risking the security or privacy of iOS ...  
22 users. Third party app stores should also be allowed to  
23 distribute apps using mechanisms of their choosing,  
24 ie their websites, without having to go through Apple's  
25 notarisation process."

1           Just pausing there, you say that is because your  
2           evidence is that third party app stores will have the  
3           incentive themselves to match or beat Apple's standards  
4           on security, privacy and safety?

5           A. Yes, that is my belief.

6           MR KENNELLY: That is a convenient moment, sir.

7           THE CHAIRMAN: How are you getting on?

8           MR KENNELLY: I am making good progress on the basis that we  
9           have a half-hour lunch break. I do have to ask for that  
10          indulgence.

11          THE CHAIRMAN: Well, I suspect probably --

12          MR KENNELLY: Depending on whether I am allowed by the ...

13          THE CHAIRMAN: Just in terms of how that looks later. I am  
14          just conscious of adding burden after burden. You are  
15          going to have to give some time for re-examination.

16          MR KENNELLY: I will, and that is why ...

17          THE CHAIRMAN: When do you plan to sit down if you get your  
18          half an hour?

19          MR KENNELLY: I will have to give you an -- I have factored  
20          in -- I have planned my cross-examination on the basis,  
21          which obviously is subject to the Tribunal, that we have  
22          a half-hour lunch break and that we can sit until five  
23          today, both of those things. Assuming that we have a  
24          half-hour break, and a ten-minute break in the course of  
25          the post-lunch period. On that basis I will finish with

1           20 minutes or so for re-examination for my learned  
2           friend and we can finish with Dr Lee today, and I really  
3           have tried to cut back. As you can see from the reports  
4           there is a huge amount of material, but on that basis  
5           I am confident that I will be finished by that time, and  
6           that will hopefully release Dr Lee at the end of the  
7           day.

8           THE CHAIRMAN: Yes. So I do not know whether half an  
9           hour -- if we are going to do half an hour at the end of  
10          the day, I am sure you do not feel good about that, but  
11          is that something you would be happy to proceed with?

12                           (Brief discussion about breaks)

13           I think what we might do is we might start at  
14          quarter to two and let us see how we go.

15           One observation I would make, Mr Kennelly, is that  
16          there is obviously the need for you to put your case.  
17          There is also, no doubt, the desire to get Dr Lee to  
18          change his views on things, but I am not sure how much  
19          progress you are going to make with that on the basis of  
20          progress to date.

21          MR KENNELLY: I understand.

22          THE CHAIRMAN: So you may feel that once you have put your  
23          case, and it is obviously a matter for you how you go,  
24          but some of it does seem to be diminishing returns at  
25          some points. Obviously you have to make that judgment.

1 MR KENNELLY: Of course. I have made the same observation  
2 myself, sir, and that will inform how I approach the  
3 rest of the submission.

4 THE CHAIRMAN: That is helpful. We will see how we go, but  
5 I think it is important that we make sure -- I am sure  
6 you do not have a view yet as to how much time you need  
7 for re-examination but it is probably going to be quite  
8 limited in 15-20 minutes. I would hope that is enough.

9 MR KENNEDY: 20 minutes would be fine, sir, subject to what  
10 comes up this afternoon, but there are only a couple of  
11 questions at the moment.

12 THE CHAIRMAN: That is helpful.

13 Dr Lee, the usual rules over lunch. Please do not  
14 discuss your evidence with anyone else.

15 A. I understand, thank you.

16 (1.05 pm)

17 (Luncheon Adjournment)

18 (1.45 pm)

19 MR KENNELLY: Dr Lee, we had just finished with your  
20 evidence that in the counterfactual on iOS, third party  
21 app marketplaces would have the incentive and the  
22 ability to implement the same kind of App Review checks  
23 that Apple does currently.

24 A. That is correct.

25 Q. Now, let us test that by looking at Google --

1 A. Okay.

2 Q. -- and how Google has struck what it thought was the  
3 appropriate balance between security and openness to app  
4 developers. Because while Google does review apps  
5 distributed through the Google Play Store before they  
6 are made available, it only began using human reviewers  
7 in 2015?

8 A. Yes, that is my understanding, yes.

9 Q. Even now, only a portion of those apps submitted to the  
10 Google Play Store are subject to human review?

11 A. Can you point me to my report where I said that?

12 Q. Second report, page 31, paragraph 50. {C2/13/31}.

13 A. Okay.

14 Q. Do you see that?

15 A. Yes.

16 Q. The Google Play Store allowed self-signed apps,  
17 I understand, until 2021?

18 A. Yes.

19 Q. Even on the Google Play Store, I think your evidence  
20 today was there was no requirement for developers to  
21 have their identity verified until 2023?

22 A. Yes, that is my understanding.

23 Q. So again looking at how Google for the Play Store or  
24 Google generally struck the balance between security,  
25 privacy and openness, can you go, please, to

1           {D1/1355/1}, please. Do you recognise this document?

2       A. Let me see. (Pause). I am not sure. Yes, I can

3       recall, sorry.

4       Q. This is a literature review commissioned by the United

5       Kingdom Government, the Department for Digital, Culture,

6       Media and Sport published in -- updated

7       in December 2022. If you go, please, to page 13.

8       A. Sorry, did I cite this reference in my report?

9       Q. I do not believe you did mention this document in your

10      report.

11      A. Right.

12      Q. Could you go, please, to page {D1/1355/13} which refers

13      at 3.3 to "App security and privacy information for

14      users". Do you see that?

15      A. I see the title, yes.

16      Q. Could you go, please, to the second last paragraph on

17      that page where it says:

18                "Apple has made a particular virtue of the security

19                and privacy of its product offer ..."

20                Do you see that?

21      A. Yes.

22      Q. Can you just read that paragraph, that paragraph alone,

23      please.

24      A. Okay. (Pause)

25                Okay, I read that paragraph, yes.

1 Q. Over the page, sorry, page {D1/1355/15}, now. The  
2 second paragraph, top of the page, please. This is  
3 contrasting Google's approach, the Google Play Store  
4 approach. If you just read that paragraph, please.

5 A. So the second paragraph, or the first?

6 Q. Just the second paragraph, please.

7 A. Okay, the second.

8 Q. The one that begins:

9 "In terms of what other app stores are doing in this  
10 space ..."

11 A. Okay. (Pause)

12 Okay.

13 Q. Do you disagree with anything in that paragraph?

14 A. Let me see the last sentence here. (Pause)

15 Okay, I mean, I agree, yes.

16 Q. So this is explaining that the Google Play Store is  
17 providing users with less information about how their  
18 data is being used, less than Apple provides in the App  
19 Store?

20 A. That is what this paragraph says, yes.

21 Q. Google made all of these choices -- I have taken you to  
22 a range of commercial decisions Google has made -- and  
23 these are choices which do not maximise security and  
24 privacy for all Android users; maximise privacy and  
25 security?

1       A. So again, I find several things. One is that I know  
2       that Android has been updating their permissions, so  
3       I would say that compared with, let us say, ten years  
4       ago, they have done a lot better. There is even  
5       teaching classes.

6                The second thing I want to say is that it seems to  
7       me, I do not know whether it is a cultural issue or not,  
8       different markets or different jurisdictions, they have  
9       different views of privacy or content, what is  
10      appropriate, not appropriate.

11               So I want to step back and say that when it comes to  
12      very obvious security violations, such as malware,  
13      I will not doubt Google is doing anything different  
14      than, let us say, Apple. When it comes to something  
15      outside the security domain, yes, a lot of -- some of  
16      these things I would say, some are subjective.

17               So it is hard for me to say which is better, as in  
18      Google versus Apple. I have different opinions in terms  
19      of somebody's contents, for instance.

20      Q. Dr Lee, you spent quite a long time this morning telling  
21      us how bad it was to allow self-signed apps?

22      A. Yes.

23      Q. Well, the Google Play Store allowed self-signed apps,  
24      did it not? That was a commercial decision taken by --

25      A. But that is in the context of allowing malware authors

1 to submit malicious app. It is different to say, oh, I  
2 submit this app just to annoy you with some content. It  
3 is very different. We say clearly that you do not look  
4 at annoying contents, you look at strict, secure  
5 violations.

6 Q. Dr Lee, you say that allowing self-signing apps is one  
7 of the major reasons why the outcomes on Android are  
8 worse than the outcomes on Apple for infections on  
9 devices?

10 A. Yes, I stand by it, because you allow the malicious  
11 authors to submit malicious apps without being known.

12 Q. The Google Play Store allowed self-signed apps on its  
13 platform?

14 A. Yes, that is a policy to me, it is a policy -- I do not  
15 want to say that is a mistake or not, that is their  
16 policy choice. Also, throughout my report I say, hey,  
17 Apple, when you open up you do not follow Android. You  
18 insist you still want developer identification,  
19 verification and app signing.

20 Q. I am just talking about incentives, third party app  
21 store incentives. Google made a choice to allow  
22 self-signed apps, and that was not a choice designed to  
23 maximise privacy and security for the Play Store users,  
24 was it?

25 A. Again, you probably need to ask a Google executive why

1 did they make that decision. But clearly I want to be  
2 reminded, or to remind myself, that we are talking about  
3 this in a context of counterfactual in iOS world, yes?  
4 So I would not think that a third party iOS app store  
5 would look at Google as a standard. Instead, they would  
6 look at App Store as the standard to follow.

7 Q. I am talking about the choices that Google is likely to  
8 make.

9 A. But why does it matter to iOS App Store who is supposed  
10 to be with the App Store instead of Google Play Store?

11 THE CHAIRMAN: You have put the point quite squarely.

12 MR KENNELLY: So turning to third party app stores more  
13 broadly, again, looking at their incentives. You recall  
14 the evidence of the third party app stores', app  
15 marketplaces', actual conduct. We saw it in the  
16 evidence this morning.

17 A. Which one?

18 Q. The National Cyber Security report.

19 A. So, again, there are many numbers being thrown around.  
20 Can you remind me?

21 Q. I am not going to -- let us just see if you can  
22 remember, Dr Lee, because it was earlier today. You  
23 remember that the National Cyber Security Report said  
24 third party app stores were typically characterised by  
25 their focus on user and developer freedom. We had

- 1 a discussion about that.
- 2 A. I thought that was referring to the Android market.
- 3 Q. Yes.
- 4 A. Okay. But we are talking about, in the context of  
5 counterfactual, the iOS world.
- 6 Q. So you think the third party marketplaces will change  
7 their incentives when they are in iOS?
- 8 A. Look, I am competing with Apple. Of course I am using  
9 Apple standard to compete with Apple.
- 10 Q. But when they are on Android they are competing with the  
11 Google Play Store, which is much better, we know, for  
12 security.
- 13 A. I have no evidence that the third party app stores in  
14 the Android world is not competing with the Play Store.  
15 I have no evidence of that either. But on the other  
16 hand, I find it hard to believe that a third party iOS  
17 App Store will use the Google Play Store as a standard  
18 to compete with Apple. It does not make sense to me.
- 19 Q. We looked at several items of evidence showing you that  
20 the third party app stores in Android typically deploy  
21 less rigorous vetting processes than the Google Play  
22 Store?
- 23 A. So again, I do not know which report you are citing, you  
24 are referencing, I think, but on all of them I challenge  
25 the conclusion. For example, vetting. What does the

1 vetting mean? Vetting means using the technical  
2 approaches to look at apps. It is vetting the users,  
3 the developers' identification and so on.

4 So, to me, I have not seen a report either cited by  
5 Professor Rubin or by your offering to demonstrate the  
6 process they have gone through to draw that conclusion.

7 Q. I showed you a GCHQ report which said that third party  
8 app stores typically have less rigorous vetting  
9 processes than Google Play Store.

10 A. But that is one paragraph that you showed me. You did  
11 not show me the process that they describe.

12 Q. I showed you the RiskIQ report and it showed you the  
13 concentration of blacklisted apps was far greater on  
14 third party app marketplaces than on Google Play Store.

15 A. So, again, they ignored the fact that they need to  
16 analyse some important factors, including the fact that  
17 they allow self-signed apps. We repeatedly talked about  
18 this multiple times.

19 Q. The NortonLifelock study showed that even the top third  
20 party app marketplaces were 19 times more likely to  
21 encounter an unwanted app as on the Google Play Store?

22 A. So again, I mean, I do not doubt the numbers that they  
23 cite. What I am challenging is that they did not go  
24 through a rigorous process to say, hey, here are the,  
25 let us say, four factors, the difference between, let us

1 say, Apple and Android or Apple and Google. Let us step  
2 through all of them, okay, one by one, to do a rigorous  
3 analysis. Then I can say, hey, which is the main  
4 factor? None of the reports did that, okay?

5 Q. So you maintain, just to be clear, that -- and I will  
6 move on now to the next point. You maintain that the  
7 third party app stores that we see on Android have been  
8 competing with the Google App Store, the Google Play  
9 Store, to maintain the same or superior levels of  
10 security, privacy and safety?

11 A. I have no reason to doubt that, because there is no  
12 report, but they contradict my belief.

13 Q. Can you show us any evidence that supports your belief?

14 A. Again, I am going to base this on my experience as  
15 a security person, a person who is very experienced in  
16 analysing apps, and so on, to tell you that, yes, if  
17 I want to operate a store, let us say App Store for  
18 Apple or Play Store in Google, what do I compete with?  
19 I compete with quality; that is common sense to me.

20 Q. We will move on to the third party app marketplaces  
21 which you say are particularly safe and secure. Can we  
22 go to your report, please, Lee 1, {C2/5/91},  
23 paragraph 168.

24 A. Yes.

25 Q. Paragraph 168, last sentence:

1           "There are therefore many safe (as well as  
2 high-quality and popular) third-party Android stores  
3 available to consumers on Android ..."

4           You name Amazon, APKMirror. You see the list?

5       A. Yes.

6       Q. Let us look at some of those.

7       A. Okay.

8       Q. Aptoide. You do not know, do you, what App Review  
9 guidelines if any Aptoide applies?

10      A. I know the Play Store guideline which is published. So  
11 as I said, if you operate a store trying to compete with  
12 Play Store, most common sense, you look at what Play  
13 Store is doing, and you do the same thing, and  
14 technically you can.

15      Q. So you think Aptoide is applying the Play Store  
16 guidelines?

17      A. So my point is that --

18      Q. Just yes or no. I am just trying to understand your  
19 evidence, Dr Lee.

20           Are you saying that Aptoide is likely to be applying  
21 the Play Store guidelines?

22      A. That is common sense. I do not recall looking into the  
23 details of Aptoide's review policy. I do not recall  
24 looking to it.

25      Q. You have no idea what kind of resources Aptoide is

1 applying to policing or enforcing any guidelines, if it  
2 has any?

3 A. As I recall, actually, I think I cited the academic  
4 paper that say Aptoide is actually the safest. So  
5 I mean, if you allow me, I can go back to that and look  
6 at the paper to say how they describe the due process.

7 Q. Let us look at what the data in evidence shows us about  
8 Aptoide. {D1/173.2/7}. This is an online review of  
9 Android stores, "10 best third-party app stores for  
10 Android", recommending Aptoide. See what it says about  
11 it. Second sentence -- sorry, third sentence.

12 A. Third sentence, okay.

13 Q. Do you see that:

14 "... the main draw of Aptoide is its looser  
15 regulations for content. You can find adult (NSFW) ..."

16 That means, I think, "not safe for work", is that  
17 right, Dr Lee?

18 A. I am having a hard time following where you ... Which  
19 sentence?

20 Q. I am reading the third sentence on that paragraph.

21 A. Okay. Starting with which?

22 Q. Starting with:

23 "However, the main draw of Aptoide is its looser  
24 regulations for content. You can find adult ... apps  
25 and games here, as well as questionable apps like

1 Show Box. Of course, this gives the app store a bit of  
2 a badlands feel, so make sure you pack an antivirus app  
3 if you use this one. Aptoide suffered a data breach in  
4 2020 ... its security ... didn't ... affect many  
5 people."

6 Do you see that?

7 A. Yes, I see the sentences. I see the paragraph, yes.

8 Q. Can I just show you {D1/1856/8}. You cited this article  
9 in your second report --

10 A. Yes.

11 Q. -- Dr Lee. For the transcript, that is footnote 207 of  
12 Dr Lee's second report.

13 Just looking at this, page 8, then the very last  
14 paragraph, please.

15 A. Are you saying I should look at my second report?

16 Q. No, I am not. I am asking you to read the last  
17 paragraph on this page, the one on the screen.

18 A. Okay, yes.

19 Q. "The content regulations are much less strict in this  
20 app store than in others. The lax regulations also  
21 affect the types of available APK app types. Expect  
22 some adult content and piracy apps that, like the other  
23 app types, you can conveniently download without having  
24 a registered account."

25 A. Right.

- 1 Q. Do you have any reason to disagree with anything that  
2 you have read so far about Aptoide?
- 3 A. No.
- 4 Q. Can we go to {D/1355}, please, back to the UK Government  
5 DCS literature review. Page {D1/1355/12}. Can you  
6 read, please, the last two paragraphs of this page.  
7 (Pause)
- 8 Do you see that?
- 9 A. I am trying to finish the last paragraph here. (Pause).  
10 Okay.
- 11 Q. So you see from this that apps are allowed on this  
12 Aptoide store even if they have not passed the malware  
13 screening process?
- 14 A. That is not what they say. They say "arguably raises  
15 the question". They do not know for sure that is the  
16 case.
- 17 Q. No, no, let us look at -- they are saying it raised the  
18 question of whether apps should be present on the store  
19 if they have not passed the screening.
- 20 A. Exactly.
- 21 Q. So there is a malware screening platform called Aptoide  
22 Sentinel. Apps that pass through this are afforded the  
23 use of a trusted app badge and the company banner.
- 24 A. Yes.
- 25 Q. It gives them like a kite mark of quality.

- 1 A. Right.
- 2 Q. That is not described as the gateway for the Aptoide App  
3 Store.
- 4 A. So --
- 5 Q. That is why the DCS report says that begs the question  
6 why apps should be getting on if they have not passed  
7 the scanning?
- 8 A. No, they say it raises the question of whether an app  
9 should be present in the store if it has not passed the  
10 scanning. Why did they not say, hey, we saw apps that  
11 have not passed scanning were present in the store?  
12 They do not say that.
- 13 Q. Doctor, will you take it from me that Aptoide allows  
14 apps on the store that have not passed the Aptoide  
15 Sentinel test.
- 16 A. Where does it say that they allow apps that have not  
17 passed any --
- 18 Q. Page {D1/1355/17}, please.
- 19 A. Okay.
- 20 Q. Page 17 at the bottom, Figure 10. This is looking at  
21 apps:
- 22 "An example from Aptoide in this case for an app  
23 that does not have the trusted app, good app guaranteed  
24 status."
- 25 A. Can it be zoomed in? Sorry.

- 1 Q. Yes.
- 2 A. Thank you.
- 3 Q. So this is showing a problem with an Aptoide app and it  
4 describes that it is an app that does not have the  
5 trusted app guaranteed status that you get when you pass  
6 Aptoide Sentinel. Do you see that? Just the first  
7 sentence of that last paragraph is all we need, Dr Lee.  
8 (Pause)
- 9 If you want to, doctor, you can read the rest of  
10 that paragraph and you can go over the page. Top of  
11 page {D1/1355/18}.
- 12 A. Okay.
- 13 Q. Now do you accept that on Aptoide there are apps  
14 published which do not pass Aptoide Sentinel and have  
15 that trusted app status?
- 16 A. Okay.
- 17 Q. If you go to page 15, please, of this document,  
18 {D1/1355/15}, final paragraph. This is about  
19 information provided to users about privacy. Can you  
20 read that paragraph, please. Read in particular --  
21 well, please read it anyway, just that last paragraph at  
22 the bottom of the page that you can see on the screen.  
23 (Pause)
- 24 A. Okay.
- 25 Q. So Aptoide is not -- sorry, do you agree or disagree

- 1 with what you have just read?
- 2 A. I have no reason to doubt what they wrote here, no.
- 3 Q. So Aptoide is not as protective of user privacy as the  
4 Google Play Store, is it?
- 5 A. I think everything I read here is about information that  
6 they failed to provide for apps that did not pass the  
7 review. But I do not know -- I mean, there is no  
8 information that they use a different standard for  
9 a privacy violation.
- 10 Q. First sentence of that paragraph, please, Dr Lee.  
11 Please read it again:  
12 "This can be contrasted ..."  
13 They just described the Google Play Store, and it  
14 says:  
15 "This can be contrasted with the level and style of  
16 information presented in the Aptoide store."  
17 Do you see that?
- 18 A. Yes.
- 19 Q. So they are comparing and finding that Aptoide is  
20 providing information in a way that the majority of  
21 users would not find meaningful.
- 22 A. But did not say the information they meant, they said  
23 a privacy violation. They just say this in a very  
24 general way.
- 25 Q. So you disagree that they are saying that Aptoide is not

1 as protective of user privacy as the Google Play Store?

2 A. What I am saying is that the information that is  
3 presented in this report did not say it, so I do not  
4 know.

5 Q. But you agree that it is saying the information is  
6 presented in a way the vast majority of users would not  
7 find meaningful?

8 A. Again, I do not want to challenge what they say.  
9 I did not do a user study, so ...

10 Q. If we go to page {D1/1355/21}, please. Bottom of the  
11 page, last paragraph:

12 "As an aside, reports in spring 2020 indicated that  
13 the Aptoide App Store itself had been the victim of  
14 a security breach, resulting in the release of data from  
15 20 million subscribers that had registered with the  
16 store ..."

17 Do you see that?

18 A. Yes.

19 Q. Were you aware of that data breach relating to Aptoide  
20 at the time of drafting your expert report?

21 A. No.

22 Q. Did you make any enquiries about the extent to which  
23 there may have been data breaches on Aptoide?

24 A. No, everybody had been hacked, including Google, so what  
25 a surprise that somebody had been hacked. In security

- 1           we say it is not if, it is when you will be hacked.
- 2       Q. You say the Apple App Store is hacked, relatively
- 3           speaking, as often as the Aptoide store?
- 4       A. It does not matter how frequent. It is not if, it is
- 5           about when.
- 6       Q. APKPure, next, Dr Lee. That was the next example you
- 7           gave of an app store you would recommend. You do not
- 8           know which or if any App Review guidelines are applied
- 9           by APKPure, do you?
- 10      A. So again, this is a while ago. I do not recall the
- 11         details of how these app stores review their apps. My
- 12         recollection is that the Amazon App Store is pretty
- 13         solid. That is all I can recall. There are so many
- 14         things I cited in my report that I cannot possibly
- 15         remember all the details of everything I cited.
- 16      Q. You recall when we looked at the NortonLifelock report
- 17         that it said that in terms of unwanted apps, the Amazon
- 18         Store was not as good as the Google Play Store?
- 19      A. I do not recall that detail, sorry.
- 20      Q. Just to show you then. I am not trying to mislead you,
- 21         doctor. I will show you the reference. It is page
- 22         {C5/246/2}. Just looking at Amazon in particular.
- 23         Left-hand column, please, second bullet point. Can you
- 24         zoom in please.
- 25                 Just near the bottom of that second bullet point,

1 speaking about alternative markets:

2 "Some like Amazon's are almost as safe as the Play

3 market ..."

4 Do you see that?

5 A. Which sentence? Okay, yes, sure.

6 Q. Do you have any reason to disagree with that finding?

7 A. No.

8 Q. APKPure, back to the other one you recommended. Can we

9 see {D1/1539.1}. Now, before we get into this document,

10 I asked you about whether they have any guidelines, and

11 you have no idea what kind of resources APKPure applies

12 to policing or enforcing any such developer guidelines,

13 do you?

14 A. Like I said, I just do not recall how I reference these

15 stores.

16 Q. Let us look at page 2 on this document, please. This is

17 a study by Avast of APKPure. {D1/1539.1/2}. You see at

18 the bottom of the page it says:

19 "You can install country-specific apps outside your

20 location, plus you can find restricted or discontinued

21 apps ..."

22 Do you see that?

23 A. Yes.

24 Q. "... and games."

25 Then:

1           "Claims to verify apps. The general lack of  
2 security protocols means that apps available on APKPure  
3 could contain vulnerabilities like malware."

4           Do you see that? Do you have any reason to disagree  
5 with that statement?

6       A. I mean, without the context of the full report, I do not  
7 know. I do not know how they say that they know that  
8 there is a general lack of security protocols. Did they  
9 say they investigate or whatever? It is different from  
10 the government report. I trust the government report,  
11 they did some study to back up some of the findings, but  
12 this report, I do not know.

13       Q. But you, Dr Lee, did not check whether APKPure had any  
14 security protocols?

15       A. Like I said, I do not recall how I checked it. I think  
16 I must have -- well, let me see. 225. Yes, I mean,  
17 I rely on this reference, 225. I cite it in my first  
18 report that talks about the ten best third party app  
19 stores on Android. So I trust this report. I mean,  
20 same as you asked me whether I should trust the report  
21 you are showing to me.

22       Q. Can we look at then, that one that you do rely on.  
23       {D1/1856}.

24       A. Okay.

25       Q. We have just looked at this, have we not?

1 A. That is what I cited in my report.

2 Q. Yes. Can we scroll to page 8, please, just to remind  
3 you. {D1/1856/8}. This we have already looked at.  
4 This is what that document tells you about Aptoide, do  
5 you see that?

6 A. Mm-hm.

7 Q. Far from telling you about its excellent security  
8 protocols, it tells you the opposite, does it not,  
9 Dr Lee? This is your document.

10 A. Where does it say it is less?

11 THE CHAIRMAN: Mr Kennelly, we have done this. We do not  
12 need to do it again.

13 MR KENNELLY: Yes, I am sorry.  
14 We are on APKPure and -- sorry, I will move on from  
15 this entirely.  
16 Let us go back to {D1/1539.1/4} just to finish that  
17 piece, because I want to show you the document, to be  
18 fair to you, Dr Lee. Do you see at the top it says:  
19 "The site may contain illegal content, cracked and  
20 pirated apps."  
21 Yes.

22 Q. It could be infringing copyright laws. Then 2021, there  
23 was an infection of Trojan malware that flooded users  
24 with adware. It was identified and a new version was  
25 released.

1           Then below that, instances like this can happen at  
2 any time because third party app stores, such as  
3 APKPure, lack the robust security offered by official  
4 app stores, like Google Play and Apple App Store?

5       A. Hold on, going back to that paragraph about flooded by  
6 ... But then they say they immediately identified, then  
7 released a new version to remove the malware, right? So  
8 my point is that even Google Play Store sometimes will  
9 get infected by -- sorry, Google Play Store sometimes  
10 also in their review they miss detecting some malicious  
11 apps which cause huge problems. So to me this is not  
12 unique to any Play Store that they miss some of the  
13 malware, and to me what this paragraph says is they  
14 could quickly identify and then release a new version to  
15 remove the malware. That is good. That means they do  
16 something about security.

17       Q. Page, D1/1539.1/5}, please. Top of the page, please.  
18 Could you read that first paragraph number 1. (Pause).

19           Any reasons to disagree with that paragraph, Dr Lee?

20       A. In the context of this report I do not know whether that  
21 means, because they are pirated apps versus -- to me,  
22 the most important thing to check for security is you  
23 check for malware. Those are the single most important  
24 thing. So I am not sure this report shed any light  
25 into, you know, that APKPure do not do a good job or do

1 not follow Google standard to check for malware. Just  
2 the fact that they miss, hey, everybody misses.

3 Q. Dr Lee, it says in terms they do not have the same  
4 security protocols, and that means there is a higher  
5 chance that the apps in APKPure could contain  
6 vulnerabilities that hackers could exploit. That is not  
7 limited to piracy, is it?

8 A. So again, when it says same security protocols, I wish  
9 they spelt out exactly what that means, and also what  
10 are the security review guidelines and rules that they  
11 are talking about here.

12 Q. {D1/1457.1}, please. Could you just read that first  
13 paragraph.

14 A. Okay. (Pause).

15 All right, okay.

16 Q. Scroll down. The last paragraph on that page.

17 A. Mm-hm.

18 Q. Just read that to yourself, please. (Pause).

19 A. Okay.

20 Q. So based on what we have seen, Dr Lee, the Tribunal  
21 cannot conclude that APKPure achieved the same levels of  
22 security, safety and privacy as the Apple App Store, can  
23 they?

24 A. Do you mean the Apple App Store? Are you talking about  
25 ...

1 Q. You said that APKPure could achieve the same levels and  
2 was achieving the same levels of security, safety and  
3 privacy as the Apple App Store; that is wrong, is it  
4 not?

5 A. No, I mean, what I said in paragraph 168 of my report 1,  
6 I talk about Android, I did not talk about Apple. When  
7 I cite Amazon App Store, APKMirror, APKPure, Aptoide,  
8 I talk about it in the context of Android, not Apple.

9 Q. 167 says:

10 "Third party app stores have comparable incentives  
11 to Apple, because to grow their business they need to  
12 provide services that will lead to good and secure user  
13 experiences."

14 By that, you meant Amazon App Store, APKMirror,  
15 APKPure, Aptoide; that is what you were referring to?

16 A. No. Look, everything has to be in the context.

17 Q. So which third party stores had these incentives?

18 A. Any third party stores, if you want to compete with  
19 Apple in the iOS world, would use -- would sort of meet  
20 Apple standards, is it not? Why would you take Android  
21 as an example to say, ah, you did not meet Apple  
22 standard. They are two different worlds.

23 Q. But they did not try to meet Google Play Store standards  
24 on Android, did they?

25 A. So, again, like I said some of this evidence -- I mean,

1 I wish somebody's report tells you, hey, they did not go  
2 through this particular technical step. That is why  
3 they are failing. I mean, to me, citing a few examples  
4 of failures of detecting some of the malicious apps, to  
5 me is almost unfair, because Google Play Store also  
6 misses detecting some of the measures out as well.

7 Q. You also cited APKMirror. Again, you do not know what  
8 App Review guidelines, if any, APKMirror applies, do  
9 you?

10 A. Like I said, I do not recall. I do not recall all the  
11 details when I went through -- like I said, my primary  
12 reference is 225.

13 Q. You have got no idea what kind of resources, if any,  
14 APKMirror applies to policing or enforcing?

15 A. I would not say that is fair. I know how App Review  
16 works --

17 Q. Just APKMirror.

18 A. No, my point is if there is an app store, I know what  
19 they need to have.

20 Q. {D1/1732/4}, please. Let us look at what this says  
21 about -- this is an article by Joe Hindy, "10 best third  
22 party app stores". He says APKMirror is not technically  
23 an app store, but rather an app repository. All kinds  
24 of stuff not available on the Play Store. It is not  
25 a full store experience.

1 A. Okay.

2 Q. You see that?

3 A. Yes.

4 Q. So again, this appears to be allowing apps that have  
5 been rejected or would not be allowed on Google Play  
6 Store?

7 A. But then you look at the last sentence:  
8 "It is surprisingly safe to use, and it is a source  
9 we often link to in our other articles."

10 Q. It is surprisingly safe to use?

11 A. Well, that means safe.

12 Q. You think that is enough to say that APKMirror provides  
13 the same levels of safety, privacy and security as the  
14 Apple App Store, do you?

15 A. Because I have no reason to say otherwise. Like I said,  
16 this 225 is my primary reference.

17 Q. APKUpdater, please. The one you recommended. You again  
18 do not know what App Review guidelines, if any,  
19 APKUpdater applies; in particular APKUpdater?

20 A. Like I said, I rely on this report, 225.

21 Q. You have no idea what kind of resources APKUpdater has  
22 applied to policing or enforcing any such developer  
23 guidelines?

24 A. Like I said, I have a sense of technically what you need  
25 to do and what you need to have. That is just very

1 common sense to people like me.

2 Q. Could we go to {D1/1732/6}. It tells us APKUpdater is  
3 not really an app store at all, but it has a neat  
4 function, you can update your existing apps without  
5 using another app store. Do you see that?

6 A. Mm-hm.

7 Q. So it is not even really an app store at all?

8 A. Yes.

9 Q. Do you agree with that, Dr Lee?

10 A. Hold on. (Pause). Yes, it is not a full-fledged  
11 dedicated app store, but it allows you to search and  
12 also update the apps that are already installed on your  
13 phone, so it is more like an app management interface  
14 which is convenient.

15 Q. So the app stores that you have listed, the evidence is  
16 clear that they do not apply the same levels of -- the  
17 same levels, as you said, of security, safety and  
18 privacy as the App Store, the Apple App Store?

19 A. So I would say that there is no sufficiently clear  
20 evidence that is the case. Like I said, all the  
21 reports, it seems to me, cited a few examples, which is  
22 not a fair comparison because, like I said, Google Play  
23 Store also fails. Also, some other nuances such as part  
24 of the apps or contents, some of these things, depending  
25 on who you ask, some of these things to me or to us in

1 security, sometimes we do not consider them as related  
2 to security violations. It can be caught by  
3 variations(?), it can be the content is not appropriate,  
4 and offensive, and so on and so forth, but we security  
5 experts look at direct security violations, so to me  
6 I would rather see reports where they analyse the  
7 security vetting steps and the techniques and then say,  
8 okay, this store is not up to the standard of Google  
9 Play. I would rather see that kind of reports.

10 Q. Let us sit back and think about incentives. You talked  
11 about incentives?

12 A. Yes.

13 Q. Is it not possible that these third party app  
14 marketplaces might be using a less stringent App Review  
15 because they do not want to incur the costs of  
16 implementing Apple's level of App Review, so it is  
17 possible, Dr Lee?

18 A. Okay, so on the other hand, my pushback is that if that  
19 results in a well known examples of bad apps, why do you  
20 think people still go there? Hey, Aptoide is known for  
21 having a ton of malware. Then why people still go  
22 there? How do they still operate and succeed as  
23 a business?

24 So to me, to say that they have incentive to lower  
25 their standards where they have more malware, can be

1 counterintuitive. I do not know how you operate this  
2 side down.

3 Q. If you have a store which has less robust vetting  
4 processes you will be more attractive to riskier app  
5 developers.

6 A. So would you operate a grocery store like that? I do  
7 not think so. Who could succeed? Hey, come to my  
8 grocery store which is cheap and also bad. Wow. I do  
9 not know. That is not in the world.

10 Q. Those app marketplaces could compete for business from  
11 developers who have been barred from the Apple App Store  
12 and they will win their business and make some money?

13 A. Okay, hypothetically, if that is the motive, then if  
14 those developers develop bad and malicious apps, why  
15 would we think the user would still go there? They will  
16 not.

17 Q. We will come back to the trust you place in users later,  
18 but in just objectionable content alone, you say that  
19 third party -- we saw you saying third party app  
20 marketplaces would have comparable or the same incentive  
21 as Apple to protect users from objectionable content  
22 insofar as appropriate. That is just not plausible, is  
23 it?

24 A. Well, I mean, the UK and the EU has a different  
25 standard. I would say the EU very much are in line with

1           what I think about objectionable content. To me the  
2           comment about EU regulation or requirement for Apple is  
3           that intuitively if there are things that are obviously  
4           bad for security, I am sure EU will ask Apple to take  
5           care of that in their notarisation. For things that EU  
6           do not check then that means the EU have a different  
7           opinion and then including some objectionable content.

8           Q. Just to be clear, when I talk about standards, I mean UK  
9           standards.

10          A. I am saying that I do not know about UK standard. Okay.  
11          So my point is the UK may have a different standard of  
12          objectionable content, but I do not think UK will have  
13          different security requirements, meaning that if  
14          something is so obviously bad for malicious purposes,  
15          I am sure UK will say yes, you should review and take  
16          care of that.

17          Q. You think some government regulation will stop it?

18          A. I believe so.

19          Q. Then you say some -- to put you an example, some app  
20          marketplaces might seek to compete for developers'  
21          business for developers who want to collect and sell  
22          user data.

23          A. Where do I say that?

24          Q. I am asking you in principle. Is that not something --  
25          you say what will these third party app marketplaces do?

- 1           They could seek to attract developers who are very  
2           interested in stealing user's data and apply less  
3           rigorous data standards than Apple.
- 4       A.   That is not how I compete.  I want to compete with  
5           quality and price.  I would not compete by doing worse  
6           things.
- 7       Q.   So you say on Android, what we see between third party  
8           app stores and Google is competition on quality?
- 9       A.   So again, I think even within Android, even Google Play  
10          Store, you could argue that they have a policy or  
11          standards about objective content and privacy different  
12          from Apple.  Now which one is better?  That is not my  
13          subject of expertise area.  But my point is that in  
14          particular, when it comes to security like malicious  
15          actions and malware, all the reports that you cited,  
16          I do not see enough evidence to say third party app  
17          stores would on purpose be using a lower standard to  
18          figure out malicious apps.
- 19      Q.   But you, Dr Lee, you have not shown us any third party  
20          app marketplace that would be incentivised to achieve  
21          the same security, safety and privacy standards as  
22          Apple?
- 23      A.   So again, are we talking counterfactual?
- 24      Q.   Counterfactual?
- 25      A.   Counterfactual does not exist here, meaning that we do

1 not have enough third party Apple App Store yet, because  
2 Apple has not allowed them to exist. The point with a  
3 counterfactual is I suppose you take away the  
4 restriction. If the question is that could a third  
5 party app store for Apple, for iOS, do the same as  
6 Apple? The answer is yes, technically, yes, and then we  
7 ask for the business incentive point of view would they  
8 do the same thing as good as Apple? Of course.  
9 Otherwise how would they compete?

10 Q. Of course, we have not mentioned developers distributing  
11 directly in the counterfactual yet, have we? We have  
12 been talking about third party app stores?

13 A. We are -- so to me --

14 Q. Here is my question, Dr Lee. Again, it is completely  
15 implausible, is it not, that developers -- all  
16 developers will be incentivised to adhere to Apple's  
17 standards of safety, privacy and security when they are  
18 distributing apps directly to users?

19 A. So first of all, I do not know, as a third party app  
20 store, why you will not require user identification and  
21 mandatory app signing? Why? Because they are competing  
22 with Apple. So to me, it's like this, if you are a  
23 developer, you say I do not want my app to be app store  
24 wide, because I can get away with worse things, why  
25 would you think the user would still go to that app

1 store? So if Apple are doing so great, why should Apple  
2 worry about third party stores stealing their business?  
3 If those third parties are not doing as well, that is  
4 again counterintuitive to me.

5 Q. Because on Android we see these developers distributing  
6 directly and they are called feral developers. They are  
7 among the worst sources of infections on Android, are  
8 they not, these developers that distribute directly?

9 A. So I do know there is evidence that they do not submit  
10 their apps to Google Play Store either.

11 Q. Take it from me, let us assume that there are many  
12 developers distributing directly on Android and they are  
13 a major vector of security, privacy and safety breaches,  
14 just assume I am right about that?

15 A. Okay.

16 Q. Why would they be any different on iOS?

17 A. So again, I think we are going back and forth. So I say  
18 on Android, because you can self-sign, to me submitting  
19 an app to a third party app store, you have the same  
20 freedom to submit that to Google Play. So that aside,  
21 on iOS, like I said, from day one, the developer has  
22 verification, revocation, signing, so to me you are  
23 talking about a different world. Android and iOS,  
24 a completely different world.

25 Q. Subject -- but their incentives would be the same on

1 Android and iOS?

2 A. What incentive are you talking at?

3 Q. The incentive, you say, to compete with the official  
4 Play Store and, you say, increase their standards of  
5 quality?

6 A. Yes, I do not know how otherwise you compete, no.

7 Q. Moving on to your fallback counterfactual, Dr Lee.

8 A. Okay.

9 Q. You say that Apple could require third party app  
10 marketplaces and developers contractually to carry out  
11 the same kind of App Review that Apple undertakes?

12 A. Where do I say that? I just want to make sure.

13 Q. {C2/5/87}.

14 A. Okay.

15 Q. Paragraph 158. You say you agree with the CMA's finding  
16 that third party app stores can be contractually  
17 required by Apple to comply with a minimum set of  
18 standards and requirements considered necessary to  
19 ensure security and quality.

20 You say you do not need the contractual obligation  
21 because third party app stores are already meeting those  
22 requirements, but your fallback is that there could be  
23 a contractual requirement to do so, yes?

24 A. Just in case, I mean, in security you can always do  
25 better by adding additional check, you know, check by

- 1           verifying. It is not nothing.
- 2           Q. Just to understand what that means, that would involve
- 3           reviewing apps against the full set of Apple's App
- 4           Review guidelines, right?
- 5           A. I think somewhere else in the report I said that Apple
- 6           can actually, how to put it, have a consortium with the
- 7           other app stores and discuss what are the sort of common
- 8           standards they can stick with.
- 9           Q. So the standards themselves could be set by some form of
- 10          industry body or industry consortium?
- 11          A. Absolutely. I mean that happens all the time.
- 12          Q. Yes. We can go back to that body in a moment. But just
- 13          in terms of how this would work, in term of applying
- 14          those standards, every app would have to be subject to
- 15          the same kind of static, dynamic and human analysis that
- 16          Apple currently applies. How else could they apply the
- 17          same standards as Apple?
- 18          A. They could say here is the thing to check. You can
- 19          deliver your own algorithms, your own methods, but at
- 20          the end, I mean, the easiest thing to enforce is to say,
- 21          hey, let us say you operate an app store, you
- 22          consistently allow malicious apps. Then people say the
- 23          percentage of malicious apps is so much higher than the
- 24          rest. I will give you time to fix it; if not, you are
- 25          out. That is actually a pretty standard thing that the

1 industry is doing.

2 Q. So when you are talking about Apple contractually  
3 requiring third parties to carry out the same kind of  
4 App Review, you do not actually mean the same as Apple,  
5 you mean App Review subject to some other standard?

6 A. What I mean is you may not need to follow the same ten  
7 weeks or same tool. But I could also say that,  
8 throughout my report I say that whatever Apple has been  
9 doing and using, those tools or whatever, are  
10 understood. So it is quite likely that any third party  
11 app store would end up developing something very  
12 similar. They may also add their own customised checks  
13 and so forth. But at the end of the day, it is about  
14 quality that can be checked and how you do.

15 Q. Before we get to the outcomes of your plan, if Apple is  
16 going to ensure that third parties are using tools that  
17 are equivalent to its tools, Apple needs to know what  
18 tools the other app stores are using --

19 A. So by tools ...

20 Q. -- to know that the contract is being honoured?

21 A. Well, I mean, I do not think the contract will say use  
22 this algorithm, but in general I could imagine the  
23 standard will say using both static analysis, dynamic  
24 analysis, human review, all of that, I mean, and when  
25 you mention those terms then it becomes very well

1           understood, because those things have been practiced for  
2           decades and people actually know how to do this kind of  
3           thing.

4           Q. But if Apple is to ensure that these third parties are  
5           conducting App Review equivalent to its App Review,  
6           Apple would need to explain to those third parties  
7           exactly what it did in its App Review, is that right?

8           A. Yes, but to me, a lot of that is actually common  
9           knowledge. It is important to say, look, Apple has a  
10          history requiring multiple third party companies, third  
11          party contribution, and there is a research contribution  
12          such as our works. My point is that the community as  
13          a whole actually understands App Review.

14          Q. But on the contrary, Dr Lee, the tools that Apple uses  
15          in App Review, many of them are highly confidential.  
16          They are the tools that we see in Mr Kosmyinka's witness  
17          statement?

18          A. Yes.

19          Q. Now, I appreciate there may be open market tools that  
20          you say are equivalent, but what Apple are using, that  
21          is highly confidential?

22          A. I think I have a supplemental report that I essentially  
23          say was a reply to the testimony by Mr Kosmyinka, right.  
24          So for every single tool that he list, I talk about what  
25          are the third party -- what actually the industry,

1 including some of the major vendors have been doing.

2 So my point is, yes, you may have your own code,  
3 instruction, but the algorithm and techniques, those  
4 things have been taught, modified (inaudible) how they  
5 analyse malware.

6 Q. So if Apple came up with a brand new technique for App  
7 Review, in order to ensure that the others were applying  
8 the same standards, they would have to share that new  
9 technique with those other third party marketplaces,  
10 would they not?

11 A. I do not know whether they would share or not. I can  
12 tell you that in computer science, in the industry it is  
13 very rare you have a breakthrough that people have no  
14 idea. It is almost never heard of. So it is more like  
15 for this platform I have some check to optimise my  
16 performance, whatever. Those things can be learned and  
17 replicated pretty quickly. The principles, no.

18 Q. Doctor, you say yourself that security is a parameter of  
19 competition, correct?

20 A. What do you mean, competition?

21 Q. Well, that --

22 A. You want to do --

23 Q. -- and that is an incentive to innovate in relation to  
24 security tools.

25 A. Yes.

1 Q. That means that if you develop something, it is very  
2 likely to be a business that is confidential to you  
3 because you want to be the best at security?

4 A. Yes, but the thing is, like I said, the breakthrough is,  
5 I do not know, once in a couple of decades kind of  
6 thing. So my point is whatever idea you come up with  
7 and then you show some result, people say, ah,  
8 interesting, now I can replicate. That happens all the  
9 time.

10 So my point is that it is almost impossible to say  
11 whatever we are doing is so secretive that nobody knows,  
12 nobody can replicate. That does not really happen in  
13 the software industry.

14 Q. I am putting to you that Mr Kosmyinka's evidence is that  
15 there are a range of highly confidential and innovative  
16 tools that Apple has developed to ensure it has the  
17 highest standards of safety and security?

18 A. So again, in my supplemental report, actually I review  
19 all of that, and also from my experience teaching,  
20 computer science, securities, software analysis.  
21 Throughout my career, including right now, I can tell  
22 you that the things we have been doing in academia in  
23 terms of cross project is far more complex and  
24 challenging than, let us say, malware. The malware  
25 author knows that you are going to analyse its malware

1           so it will do its way to obfuscate so that becomes so  
2           challenging to understand what the malware is doing. So  
3           to me, look, we know how to do software analysis for  
4           decades and decades.

5       Q. So in terms of machine learning tools, would you accept  
6           at least this basic proposition, that the more data they  
7           have -- the more data you have to train them with, they  
8           will be more effective?

9       A. In general, yes, that is a true statement, yes.

10      Q. So if we imagine a new app marketplace with equivalent  
11         machine learning tools, it is unlikely, is it not, they  
12         will be able to train that tool with the same amount of  
13         data that Apple has to train that tool with the  
14         equivalent?

15      A. Maybe not initially.

16      Q. Okay. So it depends on how much business this third  
17         party app marketplace wins from Apple?

18      A. Yes, so I think in my first report I talk about one --  
19         for example, one example of a third party app store  
20         would be, let us say, focused on games. I only do  
21         gaming apps. Actually I became very specialised in this  
22         domain, which means that maybe I have more gaming apps  
23         than, say, Apple, I have more knowledge, I can develop  
24         better heuristics, you end up actually having a better  
25         quality of review, and so forth.

1           So to me, how do you compete with Apple? You may  
2           not compete in a general App Store. You may specialise.  
3           When you specialise you can actually become very good  
4           having more relevant data.

5       Q. It depends on how much business this gaming app store  
6       wins from the App Store?

7       A. Gaming is huge and the payment is huge. Sport is huge.

8       Q. It depends on how much business you win, how much market  
9       share you win?

10      A. I do not know but I think it is very huge. Common  
11      sense.

12      Q. We move --

13      A. What do the kids do with iPhone?

14      Q. That is not anything to with the question I asked,  
15      Dr Lee. I will move on.

16      A. Okay.

17      Q. The effectiveness of your contractual obligation. Do  
18      you accept this, that a contractual obligation is only  
19      as effective as Apple's ability to check whether people  
20      are complying with it?

21      A. Yes, and I think it is very easy.

22      Q. So in order for Apple to check if other marketplaces are  
23      applying tools and techniques which are equivalent to  
24      its App Review, Apple need to audit them and look at the  
25      particular tools and techniques they are using?

1       A. I think they can request information, but also they can  
2       almost have a very direct way of doing it, because if  
3       they own iOS, they own devices, they can actually track  
4       what apps are being downloaded from where and they can  
5       track whether those apps do a bait-and-switch. So they  
6       can actually have a log of, hey, which app store is  
7       having a lot of downloads and which app store turns out  
8       to be a lot of malicious apps. So they can go to those  
9       app stores and say, tell me what you do. Why do you  
10      have so many malicious apps?

11      Q. So it depends on Apple finding out after the malicious  
12      apps have been turned up on iOS whether or not there is  
13      a problem with the quality of that review?

14      A. That is what they do right now themselves as well. They  
15      miss malicious apps --

16      Q. We will come back to information later. Because you  
17      accept, do you not, that if Apple had to conduct some  
18      kind of ongoing review, that would be quite problematic,  
19      would it not, for Apple to see exactly the tools that  
20      its competitors were using in this counterfactual?

21      A. So again, when I say contract, I did not say that they  
22      had a request -- they had to require specific tools.  
23      I think all they need to require is the capabilities.  
24      Say, hey, you should do a certain review, a certain  
25      analysis why you should scan the app code and detect an

1           obvious violation, and then if that is not sufficient,  
2           do a dynamic analysis, run the app to see whether there  
3           are some hidden behaviours. All those are requirements  
4           of the features. Exactly how you implement the tool,  
5           I do not think Apple needs to put them in contract.

6       Q. So Apple does not need to know what tools this third  
7           party marketplace is using. They could be good or bad  
8           tools, Apple does not need to know?

9       A. They do not, but I think Apple should trust that  
10           everybody knows the basic set of tools. Those have been  
11           well taught and in practice for decades.

12      Q. Let us see if in this counterfactual Apple's trust is  
13           misplaced, Dr Lee, and it turns out that there is  
14           a flood of malware coming out of these third party  
15           marketplaces.

16                Can we go to {C2/13/45}. It is the bullet point and  
17           the paragraph that begins "Third".

18      A. Okay.

19      Q. You say:

20                "... Apple and/or an industry group could implement  
21           ... standards and disallow any app store that was  
22           consistently failing to meet the standards (... by  
23           consistently approving apps that are obviously  
24           malicious)."

25                That is the standard, right?

1 A. Mm-hm.

2 Q. Now, it is clear, is it not, no such group existed since  
3 2015?

4 A. Not yet. But even CMA agrees with me, but anyway, go  
5 ahead.

6 Q. Who would be on this --

7 A. Sorry?

8 Q. This is your idea, who would be on this industry group?

9 A. Any app store, any third party app stores. Sure. Why  
10 not?

11 Q. How would it make decisions? Would it be a majority of  
12 app stores or app developers, how would it resolve these  
13 issues?

14 A. I am sure Apple probably has an outside -- I do not know  
15 how they work, but I mean, I know that Google has some  
16 kind of industry group for their app business as well,  
17 so to me industry group ... I think they want to work  
18 together, to be honest.

19 Q. You have not really given any thought as to how this  
20 industry group would work, have you?

21 A. I mean, I looked at some other somewhat relevant, let us  
22 say Google's ad technology. They actually form an  
23 industry group and then they actually publish  
24 a document, right? So the document is co-authored by  
25 a group of industry players, they have meetings and then

1           they debate and all that. So it is not like the core  
2           industry group say: I am Apple, I am the king, so you  
3           listen to me. I do not think that is how it works in  
4           industry.

5           Q. Would there be any appeals from this industry body if it  
6           decided that the App Store was consistently failing to  
7           meet standards and consistently approving apps that are  
8           obviously malicious?

9           A. Look, if there is an agreed upon standard and the  
10          standard says if you consistently fail, you will be  
11          banned by Apple, if that is an agreed upon thing there  
12          will be action taken.

13          Q. This could take some time, could it not, working out  
14          whether it is consistently failing. Is it not  
15          consistently approving apps which are malicious? Are  
16          the apps obviously malicious or not obviously malicious?  
17          This could lead to quite a lot of discussion, could it  
18          not?

19          A. Yes, that is the nature of things. Yes, maybe months,  
20          I do not know.

21          Q. All the way during this delay, the third party app  
22          marketplace is consistently approving malicious apps  
23          onto iOS, in your model?

24          A. Okay, first of all, even if that is the case, meaning  
25          the App Store has a lot of malicious apps, first of all,

1           you should not believe that there will be a lot of users  
2           going there if they know if that this app store has  
3           a lot of malicious apps. Secondly, just because there  
4           are malicious apps on this app store does not mean they  
5           are going to go there and purposely download a malicious  
6           app. So there is a reason why somebody's going through  
7           the standard, asking the fixings, it is okay.

8           Q. Even if Apple is the judge not the third party body, so  
9           it was permitted to revoke the ability of the third  
10          party app marketplace to operate?

11          A. So again, I do not think Apple needs to be the judge,  
12          right. Apple can present a law to some group and say,  
13          hey, so many users are downloading apps from this app  
14          store, these things turn out to be malicious. Maybe  
15          there will be, how to put it, other members of the group  
16          to verify, that is the case.

17                 So really my point is that these kinds of industry  
18          groups, they do not have to be -- they do not have to  
19          have a dictatorship. They could just be collaborative.

20          Q. So Apple should not be the one deciding?

21          A. Again, there are multiple ways to organise, the way it  
22          is organised, is less and less of a concern to me.

23          Q. If Apple is the one deciding, how many violations would  
24          Apple have to find? If Apple was the judge on its own,  
25          how many violations would Apple have to find before it

1 would be entitled to shut down the third party app  
2 marketplace entirely?

3 A. In the most cynical view, I would say whoever has the  
4 higher should be out. That could mean Apple itself.  
5 That would not work, because there could be apps where  
6 there is consistently absolutely no malware and then  
7 Apple looks bad. So my point is there has to be an  
8 agreed upon common sense standard that people can say,  
9 oh, that makes sense. That is verified.

10 You cannot assume that Apple has always -- has  
11 always to be the best. Maybe sometimes for some  
12 particular apps they are the worst.

13 Q. So even when Apple is the judge, it is not -- you do not  
14 contemplate it deciding on its own if the App Store is  
15 consistently approving obviously malicious apps. Apple  
16 cannot be the one who decides that under any  
17 circumstances?

18 A. So my point is that there is no need to obtain that,  
19 because such information should be available really to  
20 the public, including actually not just Apple's own log  
21 from iOS. I mean, again, and I think Dr Rubin's report  
22 says (inaudible), people do not share information. That  
23 to me is counterintuitive. Users would go online and  
24 then share their reviews of the apps in the App Store.  
25 My point is that at the point the industry group can

1 gather and say, yes, I think this app store has been  
2 consistently bad, even despite our effort to ask them to  
3 improve and so on and so forth, meaning it is not an  
4 arbitrary, unfair kind of outcome. Those things can be  
5 avoided pretty easily.

6 Q. So let us assume Apple is the judge. You can imagine,  
7 can you not, just how difficult it would be for Apple to  
8 enforce a contract like this?

9 A. I think it would be hard because, like I said, sometimes  
10 they are the worst. So Apple says, you know what, I am  
11 out. It does not make any sense to have Apple being the  
12 sole judge.

13 Q. Okay. The ability now of third parties to replicate App  
14 Review, we have been touching on it. I just want to  
15 explore that a bit more deeply, because you said now  
16 several times that third party app marketplaces would be  
17 able -- they have the incentive and you say they have  
18 the ability to implement an App Review system as  
19 effective as Apple's.

20 A. Mmm.

21 Q. We have discussed Mr Kosmyinka's statement and we have  
22 your evidence about the fact that all those tools could  
23 be replicated by a third party.

24 A. Mm-hm.

25 Q. There was one in particular, and I just want to talk

1 about this in general terms, because this is  
2 confidential and I do not want to go into a closed  
3 session. It should not be necessary for the purposes of  
4 my questions. But you saw a reference to a tool that  
5 Apple uses called Mercury?

6 A. Yes.

7 Q. For this, could I ask you to go to Mr Kosmyka's  
8 statement. I will show you only the publicly available  
9 material. It is in {B2/6/16}, paragraph 59. Do you see  
10 that?

11 A. Okay.

12 Q. You see there he talks about this dynamic analysis,  
13 because Apple uses "a grid of approximately 2,000 actual  
14 devices to launch and run iOS app submissions on  
15 physical iPhones". Do you see that?

16 A. Yes.

17 Q. You say other marketplaces could use virtual  
18 environments instead to simulate a device?

19 A. Can you point me to my report.

20 Q. Yes. {J 1/1/10}.

21 A. Okay.

22 Q. It is paragraph 17.

23 A. Yes.

24 Q. Just the first sentence, do you see that, and the  
25 second, under the bullet point?

1       A. The point on the last sentence, I want to say that I do  
2       understand that the pitfall of using only virtual  
3       environment, and they mitigate it by including physical  
4       devices, for example, I should add that actually Google  
5       from day one is actually using a lot of physical  
6       devices.

7       Q. Yes, because if you run an app in the virtual  
8       environment, the performance of the app is constrained  
9       by the limits placed on the emulator; that is true, is  
10      it not?

11      A. To me, okay, look, I do my own analysis. We actually  
12      have a famous paper, (inaudible) award. There we  
13      basically say, look, if I am now an author, if I know  
14      I am running a virtualised environment, then I know I am  
15      being analysed, I am going to change my behaviour.

16             So in that paper we say you should also include  
17      physical environment so that in case the malware, in a  
18      change of behaviour in a virtualised environment, you  
19      also have then not only in the physical environment to  
20      be sure.

21             So I am very well aware of pitfalls of a virtualised  
22      environment. On the other hand, like I said, I have  
23      experienced dealing with malware for like a whole decade  
24      with the Department of Homeland Security. We were  
25      required to process half a million samples a day.

1           So to me, if on a scale, the only way to do this  
2 actually is virtualised, and every now and then you toss  
3 a coin and say for this one I am also running physical.

4           So to me, whatever they are doing in Mercury, it  
5 does not mean that people do not know. Of course they  
6 know. They know the benefit and pitfalls and they also  
7 know how to mitigate the shortcomings.

8       Q. Let us assume that these tools, Apple's tools, could be  
9 replicated. Do you accept that for a third party  
10 operator to develop an App Review system that works as  
11 well as Apple's, they need to build a system in which  
12 these tools are integrated?

13       A. I mean, I would say that is the engineering goal, yes.

14       Q. That would be a significant piece of engineering work,  
15 would it not? You have to assess whether each  
16 individual tool is capable of operating at the scale and  
17 speed necessary to operate an efficient App Review?

18       A. So let me tell you this. When I say the DHS project, we  
19 only had two graduate students. They processed half  
20 a million samples a day. So it really depends on the  
21 talent you have. So on the other hand, also I cited  
22 Palo Alto Networks, that is a major security vendor,  
23 they hire a lot of engineers, and so on and forth.

24           My point is, yes, it is a large engineering effort,  
25 it depends really on the talent you have, but it is

- 1           really something completely doable.
- 2       Q. You say "completely doable", but this piece of  
3           engineering work may be beyond the resources of some  
4           third party app marketplaces; is that even possible,  
5           Dr Lee?
- 6       A. So I do not know. Like I cited my example of two  
7           graduate students doing it, yes, and also the whole  
8           Jekyll app took only three months, so it really it  
9           depends on the kind of people you have.
- 10      Q. Sorry, Dr Lee, are you saying that two graduate  
11           students, even the most brilliant in the world, could  
12           replicate Apple's App Review?
- 13      A. I am not saying the whole App Review, I am talking  
14           about, let us say, 2,000 devices linked together, yes,  
15           I think maybe two engineers can do that.
- 16      Q. You are focusing just on that part of it?
- 17      A. Yes, that particular aspect, yes.
- 18      Q. Coming to the efficacy of the tools, that depends on the  
19           data you have as well, does it not? For some of the  
20           tools the data is very important, the inputs?
- 21      A. I think we touched on this already, right, in particular  
22           for machine running. Yes, the more data you have, the  
23           more high quality, relevant data you have, the better,  
24           yes.
- 25      Q. But even for tools, for example, if there was a tool

1           that spots if malware reoccurs with minor variations, if  
2           you have a tool that spotted that, is it reoccurring at  
3           minor variations, the tool would be stronger if it had a  
4           bigger database of the malware that was already seen?

5           A. Yes, I agree, yes.

6           Q. A small third party or a smaller third party app  
7           marketplace will have a smaller database of previously  
8           seen malware?

9           A. So I am going to counter that, right. So the  
10          Google Play programme, a tool that you run on your  
11          Google Android phone, will actually scan all the apps  
12          you have installed, when you download a new app. It  
13          actually scans the internet on its own to find  
14          information about any new malicious apps, so (inaudible)  
15          database. My point is that it tells you that you can  
16          update your information, that you encountered samples,  
17          but also, most importantly, there is so-called data  
18          sharing on internet. Really, Google has a database that  
19          is huge. It performs internet scanning all day long.  
20          In fact, that is a well known practice in cybersecurity.  
21          You actually -- you collect(?) all these blog sites and  
22          web posting to talk about what are the latest threats,  
23          and a lot of sample codes or malware codes have been  
24          shared, for example by (inaudible). (Inaudible) is  
25          known for sharing what is actually a database of all the

1 latest malware, so I could imagine if you open up the  
2 Apple App Store distribution there is a lot of sharing.  
3 So, for example, if I download a malicious app --

4 Q. Dr Lee, we have a whole section on sharing.

5 A. -- so everybody knows.

6 Q. We are going to come back to sharing.

7 Just on the system and whether third party app  
8 marketplaces can replicate Apple's App Review. Even if  
9 they could in theory get all the tools and mimic them,  
10 they will not have the knowledge, the same knowledge as  
11 Apple has of Apple's hardware and software, will they?

12 A. So again, I find the statement hard to comprehend. Like  
13 I said, when we did the Jekyll app, which is the first  
14 academic example of how you bypass an App Review and do  
15 a bait-and-switch, we were challenged by a colleague to  
16 do something in iOS because nobody was doing it.  
17 Everybody was working on Android, because Android is  
18 open source. It took us only three months to pull it  
19 off.

20 So to me, and also given the fact that we have been  
21 doing malware analysis for a long time, I would believe  
22 that if we had wanted to open up a third party app store  
23 we could have done it.

24 Q. Dr Lee, you are not suggesting that Apple's knowledge in  
25 developing the hardware and software on which the apps

1 run does not give it an advantage in anticipating  
2 malware issues?

3 A. But what I am saying is whatever advantage they have, if  
4 you have enough talent you can overcome it pretty  
5 quickly.

6 Q. In general, third party app stores will not be able to  
7 replicate that sort of integrated knowledge and  
8 responsiveness?

9 A. So I do not know. Like I said, it took us three months.  
10 But I could count in probably my one hand similar groups  
11 in the US alone. I mean, with similar capabilities. In  
12 academia, I am not even talking about industry.

13 Q. In your reports, Dr Lee, you do not actually refer to  
14 any of this stuff about --

15 A. No, but from my experience, honestly.

16 Q. But experience that we cannot verify, can we, because it  
17 is not in your reports?

18 A. I can tell you, you can ask Dr Rubin as well. If you  
19 give a project to a PhD student, if they cannot publish  
20 a paper in a year they are going to cry. So when I say  
21 three months, a little bit faster than is usual, but  
22 normally six to nine months from beginning to end, that  
23 is what counts as a project because it is a publication.

24 So to me, when it comes to App Review, like I said,  
25 in general software analysis, it is very well known

1           stuff. So to me, I am not totally surprised that we  
2           were able to pull it off in three months.

3           Q. But you have no study, no document, nothing to support  
4           what you have just told the Tribunal, apart from --

5           A. Okay, so if you are not satisfied, I am going to tell  
6           you that the Jekyll paper was published 2013, and the  
7           next year, 2014, we published another paper that shows  
8           how you actually infect a large number of iOS devices by  
9           infecting the PCs that you sync up with. So again,  
10          between 2013 and 2014, how long? A year at most.

11          Q. The Jekyll paper that you mention. {D2/626/1}, please.  
12          This is the paper.

13          A. Yes.

14          Q. Page 2, please. {D2/626/2}. Just to show you very  
15          briefly. Second column, second paragraph, your paper,  
16          Dr Lee, do you see this:

17                 "According to the official App Review guidelines,  
18                 developers should expect their apps to go through  
19                 a thorough inspection for all possible term violations."

20                 Do you see that?

21          A. Yes, yes.

22          Q. "During this process, many reasons can lead to app  
23          rejections, such as stealing data from users and using  
24          private APIs."

25                 Do you see that?

1 A. Yes.

2 Q. Then this. You said:

3 "Although the technical details of the review  
4 process remain largely unknown, it is widely believed  
5 that such a selective and centralised app distribution  
6 model has significantly increased the difficulty and  
7 cost for malicious or ill intended apps to reach end  
8 users."

9 A. Yes.

10 Q. Do you remain of that view?

11 A. I remain so, yes.

12 Q. Back to what you say about replicating App Review and  
13 human review. Can we look at {C2/5/66}, please.

14 Firstly, paragraph 109. You say:

15 "Apple's app reviewers are not required to have very  
16 specialised knowledge. Equivalent third party reviewers  
17 can develop or acquire ... a similar level of knowledge  
18 and skills ... It is common knowledge ... My  
19 understanding is that these are well understood standard  
20 qualifications in the industry."

21 Then you say at the end:

22 "Human reviewers of third party apps can also gain  
23 more knowledge and experience through their review  
24 work."

25 Yes?

1 A. Yes.

2 Q. You accept, do you not, that Apple employs about 500 app  
3 reviewers?

4 A. I do not know about 500. I think the number I remember  
5 is 300.

6 Q. {B2/6/9}. This is Mr Kosmynka's statement. This is not  
7 confidential. Paragraph 35 first sentence, please.

8 A. Okay. All right.

9 Q. Any reason to doubt that?

10 A. No, there is no reason to doubt it, no.

11 Q. Page 11, please, in the same statement. {B2/6/11}.  
12 Paragraph 39(a), training.

13 "... dedicated training function which focuses on  
14 training both new hires within the ... organisation ...  
15 uptraining existing reviewers ...Training for our new  
16 hires last four to six weeks, and includes both  
17 theoretical, instructor-led training as well as on the  
18 job training where new hires are partnered with senior  
19 specialists who assist and walk them through the review  
20 ... generic app up dates."

21 Do you see that?

22 A. Mm-hm.

23 Q. Then ongoing training if you go to page {B2/6/18},  
24 please. Paragraph 66. Just looking at the  
25 non-confidential parts. The first sentence you see:

1           "Our reviewers are trained to look for trends,  
2           language cues, global events and other signals, all of  
3           which is collected and fed into a continual updating and  
4           training of human and computer review functions."

5           Do you see that?

6           A. Mmm.

7           Q. If you go back to page 11, paragraph 39(a), {B2/6/11},  
8           it is all overseen by a dedicated training team. We saw  
9           that?

10          A. Which sentence I should be looking at?

11          Q. It actually probably the part we already read. This is  
12          about the fact that more senior people are supervising,  
13          senior specialists?

14          A. Yes, sure.

15          Q. If you go to paragraph 37, please, (b) and (d), if you  
16          go back to page {B2/6/9}. (b), there is a policy  
17          escalations team that supports the App Review  
18          specialists to whom things can be escalated.

19                 Similarly, at (d) the non-confidential part, the  
20                 technical investigations team that receives the  
21                 escalations that require a detailed technical  
22                 investigation?

23          A. Mm-hm.

24          Q. They are assisted obviously in their review by the  
25          automated tools and information is collected for them in

1 the Magellan tool. Again, Mr Kosmynka at paragraph 63,  
2 please. That is on page {B2/6/17}. Each and every app  
3 is approved, is reviewed by the human reviewer and then  
4 the reviewer's execution inspect the app and the human  
5 reviewers leverage the Magellan tool, the proprietary  
6 app that Apple engineering developed to act as the  
7 control and orchestration for app reviewers.

8 So just stepping back, it is unlikely, is it not,  
9 that every third party app marketplace on iOS in this  
10 counterfactual have the resources in place to employ and  
11 train so many app reviewers and trainers to operate  
12 a system at that level. APKPure, Aptoide, Dr Lee,  
13 really?

14 A. So again, that is a bad example to cite, right, because  
15 it is on Android.

16 Q. It is your example.

17 A. I cite it as an example in the context of a third party  
18 app store in the Android space. So this -- I mean, like  
19 I say, they should only compete with Android Play Store  
20 using Android Play Store's standard, which Android Play  
21 Store we know, we actually talk about this, that they  
22 have human reviewers. They are the same size as the App  
23 Review in Apple. But I also know they were probably  
24 much, much earlier than Apple in terms of pushing for  
25 machine-based App Review. I know that for a fact

1           actually.

2           So again, it is a balance of how much automation you  
3           have versus how many human reviews you need to have.

4   THE CHAIRMAN:  Sorry to interrupt you, Dr Lee, but the  
5           question I think was whether a third party developer  
6           would make that level of investment.  Would they have an  
7           incentive to make the same level of investment as Apple?  
8           That is the question.

9   A.  So it may not be the same level of investment.

10   THE CHAIRMAN:  Firstly, is that a no, they would not have  
11           incentive?

12   A.  I would say they may not have to, because they may just  
13           invest in more and automatic tools, and have more  
14           success there.

15   MR KENNELLY:  So they can assume the same standards as Apple  
16           but much more cheaply?

17   A.  In fact, that is one of what Kosmynka's goals as well.  
18           If you --

19   Q.  Dr Lee, I am asking about third party app marketplaces.  
20           Your evidence is that they could do everything Apple is  
21           doing but much more cheaply?

22   A.  Not always, but I think that is a hope, or that is  
23           a possibility that they could do that.

24   Q.  It is a possibility that they could do that?

25   A.  Yes.

1 Q. It is very unlikely, is it not, that somebody is going  
2 to come in and do everything that Apple has done but  
3 significantly more cheaply in relation to safety,  
4 security and privacy?

5 A. Look, you never know --

6 Q. Apple is not throwing money away, is it?

7 A. You never know. Do you follow the news about Deep Seek  
8 from China? They use 3% of the computing power of  
9 whatever the (inaudible) model that the US is using and  
10 achieved same performance. You could never  
11 underestimate how efficiently people can view a system.

12 Q. Google has not done it. They do not lack money?

13 A. Okay, but I am talking about the Deep Seek example.  
14 They are basically -- they understand, compared to  
15 everybody. My point is if you say can it -- is it  
16 possible for third parties to develop very efficient  
17 automatic tools, I would not rule out that possibility.

18 Q. There is no evidence for the Tribunal to suggest that  
19 any other app store or platform operator has been able  
20 to engineer an App Review system which is as effective  
21 as Apple's?

22 A. So we are talking about counterfactual world.

23 Q. On the factual world right now.

24 A. Factual world, there is no third party Apple App Store  
25 that I know. Yet even Mr Federighi said it is too early



1           Then I said "and distribution", but I think  
2           I overspoke Dr Lee, and it was not -- that part of my  
3           question was not caught. But just for the avoidance of  
4           doubt, that was part of the question too.

5       THE CHAIRMAN: Yes.

6       MR KENNELLY: Then Dr Lee disagreed.

7       A. You mean centralised system or App Review, you should  
8           have said centralised system for app distribution?

9       Q. Of App Review and distribution.

10      A. Okay, fine. Yes, thank you.

11      Q. But I recall saying that as you were speaking.

12      A. Sorry.

13      Q. It was entirely my fault.

14      A. Sorry.

15      Q. Entirely my fault, Dr Lee.

16           Now we are turning to this question of users,  
17           because a few times today you said, well, users would be  
18           able to differentiate between safe stores and safe apps,  
19           differentiate then from malicious ones?

20      A. Mmm.

21      Q. If you go to your second report, paragraph 97. This is  
22           {C2/13/57}. You say:

23           "Users are already used to making security-related  
24           decisions on other devices and, if necessary, would be  
25           able to make security-related decisions on their iOS

1 devices."

2 Over the page, whether to use a particular App  
3 Store, for example, they are able using web browsers on  
4 the iOS device.

5 Skipping ahead:

6 "Users are generally able to exercise the  
7 appropriate level of judgment as to whether or not to  
8 choose to access particularly websites based on factors  
9 such as reputation and appearance."

10 Then you say:

11 "Users in the counterfactual would similarly be able  
12 to exercise such judgment when deciding whether to  
13 download an app from an alternative app store or  
14 directly from the developer's website."

15 As such, you say:

16 "... I do not consider that there would be  
17 a considerable additional risk in the counterfactual as  
18 compared with the actual world."

19 Could I take you to the Zimperium report again which  
20 you cited in your report.

21 A. Okay.

22 Q. {D1/1368/25}. Under the heading, "The proliferation of  
23 supply chain attacks". Could we zoom in on that,  
24 please.

25 Second paragraph:

1            "These attacks are particularly effective in the  
2            realm of mobile apps due to several key reasons. First,  
3            there is a high level of trust and legitimacy associated  
4            with components within the mobile app supply chain, such  
5            as [we see] app stores, making it easier for attackers  
6            to infiltrate and compromise them. Widespread  
7            distribution of mobile apps ... and the complex and  
8            interconnected nature of the app ecosystem makes it  
9            challenging to detect such attacks, because the  
10           compromised components can appear genuine and evade  
11           automated security checks."

12           Do you see that?

13           A. Mm-hm.

14           Q. Do you disagree with that statement? Anything in that  
15           paragraph you disagree with?

16           A. I think this actually does not talk about the average  
17           users, it is more talk about the supply chain that  
18           affects the development of the apps, I think.

19           Q. It is a high level of trust and legitimacy that users  
20           have in app stores, and that is what makes it easier for  
21           attackers to infiltrate and compromise them because the  
22           users trust them?

23           A. Okay, so what I am trying to say is that the second  
24           sentence refers to: there is a high level trust and  
25           legitimacy associated with components with a mobile app

1 supply chain.

2 So by mobile supply chain, the way I understand  
3 normally is, for example, the libraries the mobile app  
4 will use. I am sure this is probably referring to the  
5 famous example of Ghost X, you know, the famous example  
6 of people downloading the library from a third party  
7 website that essentially violates some basic security  
8 rules. Normally we say, let us say, Apple, when you  
9 publish, let us say, X code, you should also publish  
10 a hash code.

11 Q. Dr Lee, it says "app stores" in the sentence.

12 A. Yes. So again, the Ghost X attack is any app developer  
13 using the library gets infected, and when they upload it  
14 to Google's -- Apple's App Store people just get  
15 infected.

16 Q. Dr Lee, you can disagree if you disagree that there is  
17 a high level of trust and legitimacy associated with app  
18 stores?

19 A. Yes, including Apple's App Store.

20 Q. All app stores; it is not distinguishing?

21 A. Yes, so, I mean, sure. I mean people -- so my point is  
22 that trusting Apple's app's store is no different from  
23 trusting an otherwise reputable third party app store.  
24 It is based on --

25 Q. The same document, Dr Lee, page 29, please.

1 {D1/1368/29}. Hopefully this is clear enough:

2 "Users Fall for Mobile Phishing ... Period:

3 "Simply put, mobile phishing works. The average  
4 user will tell you that they receive many phishing texts  
5 and emails, but they never fall for them. Zimperium  
6 data says otherwise."

7 Then they describe how an average of four malicious  
8 phishing links clicked for every device covered with its  
9 anti-phishing technology. Do you have any reason to  
10 disagree with that?

11 A. So again, phishing in general is pretty, how to put it,  
12 a pretty major threat vector, but I do not know whether  
13 this report is specific on Android versus iOS.

14 One thing I wanted to point out is that the  
15 Kaspersky report that we mentioned on Thursday about  
16 objectionable content, I double checked on the weekend,  
17 that was on Android, not on iOS.

18 So the point is that if somebody is phishing  
19 objectionable content, they do not result in malware  
20 downloading, because iOS would not allow a malware to be  
21 automatically downloaded.

22 Q. We are in the counterfactual now, Dr Lee. Take it from  
23 me there is a greater risk of malware. My focus is on  
24 whether the users can be trusted to spot problematic  
25 apps, and this report says no.

1       A. So even in the counterfactual, iOS would not allow any  
2       software, including malware, to be automatically  
3       downloaded. The user has to initiate the action to  
4       download. Even on Android now, the browser would warn  
5       you and say, hey, this is from an unknown source. The  
6       user has to go to settings and say, I do not care, trust  
7       the source.

8               So my point is some of these threats of content  
9       phishing can be overblown and you say that would result  
10      in automatic downloading of malware. Not so fast. Both  
11      iOS and Android will stop that.

12              Now, if you say, hey, here is an app that displays  
13      objectionable contents and also then change in  
14      behaviour. That to me is a generic bait-and-switch.  
15      Nothing to do with --

16      Q. I am not talking about --

17      A. The same thing as phishing.

18      Q. Phishing, let us assume that it is dealing with malware.  
19      Let us assume that this phishing attempt on iOS in the  
20      counterfactual contains malware. Let us assume malware  
21      has got through, it happens?

22      A. Okay, yes.

23      Q. Users fall for that kind of phishing, do they not?

24      A. Okay, even if you click a link, even if the link  
25      attempts to download malware, iOS will stop it, like

1 I said, by design.

2 THE CHAIRMAN: Dr Lee, that is not the question, I do not  
3 think. We understand what you say about that. The  
4 question simply that you are being asked is whether you  
5 accept that mobile users will fall for phishing. That  
6 is the question, simple as that.

7 A. Okay. In that case the answer is yes, any user on any  
8 platform will fall for phishing.

9 MR KENNELLY: Thank you, sir.

10 Page 64 {D1/1368/64}, under "Third party app  
11 stores". Third paragraph. Could you read that  
12 paragraph, please?

13 A. Okay.

14 Q. Just the third paragraph. (Pause)

15 A. So I am a little bit confused. Are we talking about  
16 iOS?

17 Q. They are talking about -- no, they are talking about  
18 Android, because they are talking about the third party  
19 app stores.

20 A. So again, I studied Android as well. Android will warn  
21 you, where you are downloading from a known source, or  
22 you are actually authorised to download it from there.  
23 So for somebody's phishing thing to check you from one  
24 side to the other, that really counters what  
25 I understand what Android is doing.

1 Q. So you disagree, where it says:

2 "Often users lack an understanding of the potential  
3 danger they are subjected to."

4 A. I do not disagree with that, meaning that some users may  
5 still go ahead and download from a particular third  
6 party store or website even though Android warned them,  
7 right? So that is -- yes, but like I said, automatic  
8 downloading malware is a thing of past.

9 Q. {D2/1039/4}. This is now smishing, so it is the attacks  
10 that are delivered by traditional text messages and  
11 non-SMS messaging apps.

12 A. Yes.

13 Q. Do you see first paragraph:

14 "These attacks primarily spread uninterpreted and  
15 unnoticed due to their deceptive nature."

16 Who is being deceived, Dr Lee?

17 A. Look, let me tell you the answer. The users, I mean, I  
18 tell you that during the political campaign cycle, every  
19 day I get a submission on the message app of Apple  
20 telling me to donate money to some particular party.  
21 All I could do is report junk and delete. You know what  
22 I got the next day from a sender that claims -- the  
23 sender's name is You Cannot Stop Us. That is their  
24 name. Is it not offensive? My point is smishing attack  
25 happens all the time, even on the message app of Apple.

1           So I do not know what to say about this. Yes, it  
2 happens.

3 Q. But the point is about whether users can spot the  
4 problem.

5 A. I spotted it. That is why I say report junk, and then  
6 it came back and say You Cannot Stop Us, too bad.

7 Q. I am talking about users generally.

8           Second paragraph:

9           "Smishing deception is enhanced due to users having  
10 false confidence in text message safety."

11           Do you agree or disagree with that statement?

12 A. Can you tell me again which?

13 Q. It is the second paragraph. It is a single-sentence  
14 paragraph.

15 A. So, I mean, I studied smishing quite a bit and phishing  
16 quite a bit. I can tell you that most people would tell  
17 you that everybody would fall for some phishing, in  
18 particular some spear phishing. I made a study of  
19 Facebook --

20 THE CHAIRMAN: Dr Lee, I think your answers are getting very  
21 long, and Mr Kennelly is really just trying to establish  
22 some very basic points with you, which is whether you  
23 agree with some of these observations that are made  
24 about users' propensity to accept this material. That  
25 is all he wants to know from you. We understand you

1           have all sorts of views about other protections, and so  
2           on, but that is not what he wants at the moment. So if  
3           you can keep your answers short, that would be helpful.

4           A. Thank you for your reminder. Could you repeat your  
5           question again?

6           MR KENNELLY: Do you agree with the second paragraph or not?

7           Yes or no. Or I do not know, that will also do.

8           A. Yes, I do not know. I do not know the (inaudible).

9           Q. {D1/1371/6}, please. This is another report that again  
10          you relied on, Dr Lee, and it is {D1/1371/6}. This is  
11          the MSI Verizon report from 2023. Page 6 tells you  
12          about security breaches, and if I could ask you, please,  
13          to go to page {D1/1371/7}, dealing with the users'  
14          ability to spot problems, users and behaviours, and it  
15          tells you, under the "Complacency Problem":

16                 "Despite improvements in cybersecurity training,  
17          many users are not well informed about the risks  
18          associated with mobile devices. Nearly half of users  
19          think that clicking on a malicious link or opening  
20          a malicious attachment can only affect their device."

21                 Do you have any reason to disagree with that  
22          statement?

23          A. No, it points to human weakness, same as human  
24          reviewers.

25          Q. The next paragraph explains why over a third have fallen

1           for one of the five following basic security errors; do  
2           you see that?

3       A. Can you scroll down a little bit.

4       Q. Can you read the rest of the page, please. Any reason  
5           to disagree with that data?

6       A. No.

7       Q. Page {D1/1371/8}, please. This again is dealing with  
8           the same problem about why we cannot count on users to  
9           spot problems, "The danger of security fatigue".

10      A. Okay.

11      Q. Again, have you any reason to disagree with that  
12          statement?

13      A. Let me see. Which paragraph you want me to read, or you  
14          want me to read the whole page?

15      Q. Just the first paragraph. It is a phenomenon which the  
16          report you cited refers to, the danger of security  
17          fatigue. (Pause)

18      A. Yes, I mean, I think my report also talks about  
19          mitigation to this kind of fatigue.

20      Q. We will come back to mitigation.

21           Page 11, please. {D1/1371/11}. Again, users are  
22          not as savvy as they think, says the report, tracking  
23          the awareness of cybersecurity among users.

24           "Users say all the right things ..."

25           But then skipping down:

1           "The evidence shows otherwise ...

2           "The data shows that 53.2% clicked on the link in  
3 a simulated targeted phishing attack.

4           "Attackers continue to rely on phishing because it  
5 works."

6           Do you see that?

7       A. Yes, I see it.

8       Q. Any reason to disagree with that?

9       A. I think 53.2 is too high.

10      Q. Have you done any study of your own to contradict that  
11 one?

12      A. I talk to CSOs. Normally they say a single figure like  
13 4 or 5%. Any organisation --

14      Q. Can you point, Dr Lee, in your vast experience, to any  
15 study, anything, that says only 4 to 5% of people fall  
16 for phishing attacks?

17      A. I do not have anything off the top of my head. But if  
18 you search for phishing training, most organisations do  
19 that, that rate goes down drastically.

20      Q. Page {D1/1371/12}, please. Again, dealing with  
21 phishing. Can I just -- can I draw your attention to  
22 the quote in the black box on the left-hand side. It  
23 seems:

24           "The mobile device presents a fundamentally  
25 different environment from a laptop or desktop."

- 1                   Do you see that?
- 2       A.   Yes.
- 3       Q.   Read the rest of that paragraph, please, that quote.
- 4                   (Pause)
- 5                   As a general statement, do you agree or disagree
- 6                   with what Mr Cockerill is quoted as saying there?
- 7       A.   I do not know what to say. That is very different from
- 8                   how I use my smartphone so I do not know. I have no
- 9                   opinion if that is what he said. Did he actually cite
- 10                  any user study, industry report, so-and-so forth? Does
- 11                  not seem to be.
- 12       Q.   Page {D1/1371/13}, please. Right-hand side. Could we
- 13                  zoom in on the block box on the right-hand side.
- 14                  There is reference here to:
- 15                  "The growth of artificial intelligence ..."
- 16       A.   Okay.
- 17       Q.   "... creating deep fake images and videos. This makes
- 18                  phishing attacks even more effective."
- 19                  Do you see that?
- 20       A.   Yes, again it depends on the context. We actually
- 21                  studied deep fake as well, yes.
- 22       Q.   So you agree with the general propositions being
- 23                  advanced here?
- 24       A.   It really depends on context.
- 25       Q.   You have no reason to doubt it, you have got nothing to

1 show us that this is wrong?

2 A. Like I said, it depends on context. Like I said, you  
3 say, hey, Wenke I saw you in this place. You know that  
4 is not the case, or your friend is not there, you kind  
5 of know it is a deep fake. In particular, also, you  
6 have used deep fake to do a live authentication.  
7 (inaudible) virtually had a whole survey paper on that.  
8 But on the other hand, you say, hey, here is Tom Cruise  
9 jumping out of this building. People say, oh, maybe  
10 that is true.

11 So really it depends on the context, meaning that  
12 the more you know about the context of that video, the  
13 more chance you know if it is deep fake or not. Anyway,  
14 that is almost off-topic.

15 Q. Yes. But sticking with the topic, Dr Lee, the reality  
16 is, let us see if you can agree with this, if the number  
17 of problematic apps that are made available increases,  
18 it is likely that the number of such apps being  
19 installed will also increase?

20 A. Okay, but remember security is always a cat and mouse  
21 game. Just because the attacker had been improving the  
22 quality of the deep fake, the countermeasures are also  
23 being developed and deployed as well, so ...

24 Q. We cannot count on users to stop the apps being  
25 installed if they are problematic, can we?

- 1 A. I am saying that countermeasures will be the App Store  
2 when they review it.
- 3 Q. Sorry, just please answer my question about users before  
4 we talk about countermeasures.
- 5 A. But the App Store review affects the user, is it not, if  
6 the App Store review rejects the app.
- 7 Q. If the app is available on the App Store and it is  
8 problematic, can we count on the users to not download  
9 it because they will spot the problem? Just that,  
10 Dr Lee.
- 11 A. So, again, it depends on context. Some users are better  
12 than others. Depends on application. Whether the user  
13 would even download it or not. I mean, again --
- 14 Q. In general, can we count on users to spot problematic  
15 apps and not download them, based on what you have seen  
16 in the material I have shown you?
- 17 A. Again, I think it depends on the sophistication of the  
18 attack and contents. It is the same challenges faced by  
19 the human app reviewers.
- 20 Q. {D1/1355/1}. This is a literature review from the  
21 United Kingdom Government, DCMS again, page  
22 {D1/1355/29}, please.
- 23 Just before I get into this, Dr Lee, by reference to  
24 your last question, you said app reviewers, the trained  
25 experts often miss things.

1 A. Yes.

2 Q. How then can ordinary users in general be expected to  
3 spot problems, problematic apps, and not download them?

4 A. So again, it depends on context, right? So --

5 Q. Dr Lee, just in general. Think about what you are  
6 saying. Obviously they cannot be if the app reviewers  
7 are missing them?

8 A. So again, I think for the most sophisticated ones  
9 I think they are going to be missed by everybody.

10 Q. In general?

11 A. Yes, in general, the most sophisticated ones, yes.

12 Q. Just to give you the full picture, page 29 is in front  
13 of you. Can you zoom in at the top, please. It is the  
14 paragraph above "Recommendations".

15 A. Which paragraph?

16 Q. The paragraph above the word "Recommendations".

17 A. Okay, yes.

18 Q. Just read that to yourself, please. (Pause).

19 A. Yes, I finished reading, yes.

20 Q. Have you any reason to doubt those figures?

21 A. I would say this on Android, and Android had actually  
22 changed how they gave permissions after those years, in  
23 fact now so-called first use. Even though an app has  
24 permissions that have been approved by App Review, they  
25 would still insist that the app would ask the user the

1 first time they used that permission. Actually, it is  
2 a response to this report, I would say.

3 Q. So we are moving on to fragmentation of information.

4 A. Okay.

5 Q. Our case that the fragmentation of information reduces  
6 Apple's efficacy, Apple's App Review efficacy.

7 So just to try some very basic things. If  
8 developers can distribute their apps through multiple  
9 different sources, Apple will have less visibility  
10 overall than it has currently over the sorts of  
11 security, safety and privacy challenges facing users?

12 A. If you point me to my report, I think I discuss --

13 THE CHAIRMAN: I think, Dr Lee, it is just a general  
14 principle. Either they do or they do not.

15 A. So as a general principle, I do not agree with that  
16 statement, no.

17 MR KENNELLY: So there is no reduction of visibility overall  
18 where apps have been distributed through multiple  
19 different sources.

20 A. I think it is Apple's choice to have that information or  
21 not.

22 Q. Because Apple can require them to provide it to it?

23 A. Absolutely. Also --

24 Q. We will come to that.

25 A. Yes.

- 1 Q. But if, take it from me, Apple has less information  
2 overall and less information, let us put it this way,  
3 less information as -- less immediate information?
- 4 A. Okay, what do you mean by "immediate"?
- 5 Q. Okay, let us just say less information. Let us assume  
6 Apples gets less information where apps have been  
7 distributed through multiple sources, just assume I am  
8 right. If that is the case, they would have less  
9 information to train their automatic -- automated review  
10 tools, is that not right?
- 11 A. Yes. But like I said, iOS can essentially log  
12 everything. It knows everything immediately.
- 13 Q. It would have less information available to its human  
14 viewers when they were trying to spot copycat techniques  
15 or apps?
- 16 A. That is not true. iOS can detect a malicious app has  
17 been downloaded from, say, a third party marketplace.  
18 iOS can in principle send it to app store and let the  
19 human reviewers play with it. But at the end, that is  
20 a choice by Apple. They can do it. Technically and  
21 whatever thing they can do, they are the vendor, they  
22 are the sole owners of the OS, so they can do  
23 everything.
- 24 Q. So Apple can sweep its system at particular times and  
25 try and spot these apps on --

1 A. Absolutely. Everything we have here, Apple can know if  
2 they want to.

3 Q. That is ex post facto sweeping by Apple?

4 A. I am sorry?

5 Q. After distribution?

6 A. Yes.

7 Q. Sweeping by Apple?

8 A. Yes.

9 Q. If --

10 A. Hold on. But Apple can also pretend to be a user and  
11 download every single app from every marketplace. That  
12 is actually standard practice in security. You play  
13 a monkey in a way, just click everything.

14 Q. Again, that is spotting apps after they have been  
15 distributed?

16 A. After it is on the App Store, yes.

17 Q. Apple will have less information from user reviews,  
18 won't it, if there is a decentralised distribution  
19 model?

20 A. I disagree.

21 Q. Well, the users are not going to leave reviews on the  
22 App Store, are they, when they download apps from third  
23 party app marketplaces?

24 A. Why should they doubt that? Why would they not review  
25 just because from a third party app store? Why would

1           you doubt that a third party app store marketplace will  
2           not let user review?

3       Q.   Is your evidence that a user on a third party app store  
4           that has a problem will leave the review on the Apple  
5           App Store?

6       A.   So again, like I said, it is Apple's choice of finding  
7           information. They can pretend to be a user, go into  
8           a third party marketplace, download all the apps and do  
9           all the reviews if they want to. What is stopping them?

10      Q.   So it requires Apple then to go and read all the reviews  
11           already published on the third party app store?

12      A.   Same way as they are reading all the reviews on the App  
13           Store now. What is the difference?

14      Q.   You accept that Apple needs that information, the  
15           information about problems after distribution, because,  
16           for example, bait-and-switch apps only reveal their  
17           harmful nature after they have been downloaded?

18      A.   I think, in principle, the more information the better.

19      Q.   Now, turning to user reviews. Unless Apple is getting  
20           user reviews from every single third party app  
21           marketplace which provides user reviews, it is going to  
22           have less information than it has currently?

23      A.   I do not have a reason to think that way, no.

24      Q.   Another type of information apart from user reviews that  
25           is important is patterns in download and purchase

1 transaction data. So looking at download and purchase  
2 transaction data, patterns that emerge there is also  
3 important for security, is it not?

4 A. Yes, but iOS can track that information as well.

5 Q. But if Apple is not the sole source by which apps are  
6 downloaded and purchases facilitated, it is not going to  
7 get that information automatically, is it?

8 A. It is automatically on iOS, they could do it.

9 Q. They would have to get it from the third party app  
10 stores?

11 A. No. When you download an app from a third party  
12 marketplace, iOS knows that; iOS -- if Apple is so  
13 willing then the information can be shared back to Apple  
14 right away.

15 Q. But that still requires the third party app store to  
16 share the information with Apple?

17 A. I do not understand your statement there.

18 Q. If the third party app store is distributing the apps,  
19 Apple is not cited on each and every app that that third  
20 party app store is distributing to its customers?

21 A. But the thing is when you download an app to iOS, iOS  
22 knows where the app is coming from. That is my point.

23 Q. Yes, but the extent to which problems arise is not  
24 communicated automatically to Apple, is it?

25 A. I do not know what information you want, but like

1 I said, the fact that the app is downloaded from a third  
2 party marketplace can be -- is known to iOS, iOS can log  
3 that, and then if -- when the app runs, any security  
4 violation, the same on-device mechanism can detect it.

5 I said this throughout my report.

6 Q. Apple would have to run that app after its download,  
7 what, continually to see if a problem arises?

8 A. Look, if the app is downloaded to your device, you as a  
9 user do not run it -- it does not matter. But whenever  
10 you run it, iOS can basically log the information. So  
11 iOS will not have to run your app automatically, just  
12 wait for you to run it.

13 Q. When an app is run by the user, if a problem arises  
14 Apple will be automatically notified?

15 A. That is doable, absolutely.

16 Q. It is doable, but it would require communication between  
17 the third party app store --

18 A. No.

19 Q. Well, it would -- between the app and Apple.

20 A. In this case it would be the device and Apple.

21 Q. Yes.

22 A. Like I said, Apple can do it. Whether they are willing  
23 or not, that is a different discussion that I am not  
24 expert in.

25 Q. It would require some new technology, would it not?

- 1 A. No.
- 2 Q. But Apple would not currently be notified of -- for  
3 example, let us talk about the DMA, for example. Where  
4 an app is downloaded and a problem arises, a malicious  
5 app, Apple does not automatically discover that  
6 a problem has arisen on that app?
- 7 A. So, again, it depends on --
- 8 Q. Yes or no, Dr Lee?
- 9 A. It depends on the nature of the attack. If the nature  
10 of the attack violates Sandboxing rules, of course iOS  
11 detects it immediately, but there are always very  
12 sophisticated malicious apps that just evade all your  
13 detection.
- 14 Q. If it was a social engineering problem, Apple has no  
15 idea that it has happened?
- 16 A. So I want to add that if we talk about social  
17 engineering content, sure, that is an in-your-face  
18 thing. But when it comes to actually doing something  
19 bad, normally that is the app's interaction with your  
20 device or iOS. So right there, the iOS will have  
21 a chance to know what is going on, whether through  
22 social engineering, objectionable content or whatever,  
23 but say, hey, you do something bad, iOS can detect that.
- 24 Q. Patterns in download and purchase transaction data.  
25 Again, if Apple is not the payment provider, it does not

1 know what apps are being -- what money is being spent,  
2 what purchases are being made, does it?

3 A. It does not know. But again, like I said, if they are  
4 so willing to determine, they could figure it out, like  
5 I said. I mean, Apple has a ton of money. Why can they  
6 not just pretend to be a user and download all the apps  
7 and see what happens? They could, every day.

8 Q. Download all the apps and make all the purchases?

9 A. Yes.

10 Q. What about a spike in refund requests?

11 A. To me, those are minor things. To me, that is a minor  
12 thing to Apple. They have so much money. If security  
13 is so important, they should pay for it.

14 Q. You mean get it from the third party app stores and the  
15 third party payment providers?

16 A. Meaning that if they want to know this so badly and a  
17 third party app store will not give away information,  
18 there are many ways Apple could do to find the  
19 information.

20 Q. Let us see about that, but just assume from me that if  
21 Apple does not get all those refund requests it is going  
22 to have less information of that kind, the patterns that  
23 can be identified from spikes in refund requests?

24 A. So again, I think to me as a security researcher,  
25 I would just say it is so possible, if they are so

1 willing, to figure out what is going on with third party  
2 marketplace. We are doing this kind of research all the  
3 time. We trawl the web, we click everything, pretend to  
4 be a user to see what is happening. I mean, yes, like  
5 I said, I maintain that Apple could find out all the  
6 information they need to find out.

7 Q. The key thing I think you are saying, Dr Lee, is that  
8 the third party app marketplaces and developers would  
9 share information about problems like malware. You say  
10 in your reports that if problems arose, they would share  
11 that with Apple?

12 A. I do not see why not.

13 Q. Well, first of all, it depends a bit on how good these  
14 third party app marketplaces are at spotting problems in  
15 the first place, their ability to identify malicious  
16 apps?

17 A. Yes, that also goes -- the same goes with the Apple as  
18 well, right? Everybody would fail at some point. The  
19 point of information-sharing is a good practice. People  
20 do information-sharing. Why? You also benefit from  
21 information that is shared by others, so you are sharing  
22 information to benefit others. That is a common  
23 practice.

24 Q. Based on the data we have seen, many of these third  
25 party app marketplaces do not seem to be very good at

- 1           spotting problems?
- 2       A. I think you are citing an example that is not in the iOS  
3           world, so ...
- 4       Q. Obviously, because there is not one. But on Android,  
5           the data shows that many third party app marketplaces do  
6           not seem to be very good at spotting problems in the  
7           first place?
- 8       A. But I think we went through this, right? I think there  
9           are a lot of other factors, including the lack of  
10          developing identification and allowing self-signing  
11          apps, and so on and so forth. So it is not necessary  
12          that their reviewing process or method is poor, is less  
13          effective, it is quite possible that their policy of  
14          allowing a self-sign app actually allows more malicious  
15          apps being submitted, and then third party is not  
16          perfect, and they end up having more malicious apps.
- 17      Q. You agree that user reviews are very important for  
18          keeping the platforms aware of malicious apps?
- 19      A. I do not have a particular opinion. I do not read user  
20          reviews.
- 21      Q. Again, this is your area of expertise. You have a view  
22          or not. Are user reviews important in identifying  
23          malicious apps or not?
- 24      A. I would say malicious apps, yes.
- 25      Q. Social engineering?

1 A. Social engineering, I mean, anything that is bad to the  
2 user, I imagine they share that in the review, yes.

3 Q. But not all third party app marketplaces have user  
4 reviews?

5 A. I do not know as a fact. I also do not know why.

6 Q. Well, you take it from me that not all third party app  
7 marketplaces have; does that mean -- does that sound  
8 right to you, they do not all have them?

9 A. I do not know for a fact that some of them do not  
10 provide user reviews. I do not know that is a fact.

11 Q. {D1/1355/17}, please.

12 A. Can you zoom in, please?

13 Q. It is under using "Community insights".

14 A. Okay.

15 Q. "In addition to what app developers declare about their  
16 wares, some app stores also offer a further route for  
17 potential users to learn about security and privacy  
18 issues ... the reviews that have already been posted ...  
19 stores vary in whether this facility is offered ... the  
20 official stores do so ... Third party stores are more  
21 variable ..."

22 Do you see that?

23 A. Yes, variable, they say "variable", yes.

24 Q. The quality of the user reviews will vary too, will they  
25 not, because some user reviews may be thumbs up, thumbs

- 1 down. Others may have more text?
- 2 A. So again, it really depends on the user base. Are you  
3 saying you reviewed the restaurant. If it is only like  
4 20 people reviewing you should probably avoid the  
5 restaurant.
- 6 Q. Also --
- 7 A. Yes, you can trust them. So my point is some of  
8 these -- the amount of reviews I would say that really  
9 depends on user base, how big the user base is.
- 10 Q. Is it also very important, Dr Lee, that the user reviews  
11 are themselves vetted because there may be many fake  
12 user reviews especially if there is a malicious actor?
- 13 A. I agree that is why I do not trust any review with only  
14 20 people.
- 15 Q. But for information sharing you have not offered us any  
16 evidence that third party app marketplaces actually do  
17 vet their user reviews today on Android?
- 18 A. I have not looked into that problem specifically.  
19 I have no reason to believe that is not the case, that  
20 third party app stores or Google Play do not read their  
21 reviews and try figure out what is going on. Yes.
- 22 Q. So you say for Aptoide, APKPure, the others we looked  
23 at, you say you have no reason to think that they do not  
24 all properly vet their user reviews to the extent they  
25 have any?

1 A. I do not know vet. This is just read them.

2 Q. Lee 2, please, your second report. {C2/13/26}.

3 A. Okay.

4 Q. Paragraph 41. About halfway down the page you say:

5 "Further, there is no reason that third party app

6 stores would not share information about malware because

7 information sharing is a standard practice in the

8 industry already."

9 Do you see that?

10 A. Yes.

11 Q. Do you see the footnote you give for that?

12 A. Mmm.

13 Q. The US Cybersecurity & Infrastructure Security Agency.

14 Will you take it from me, Dr Lee, that that document you

15 cite does not say anything about whether third party app

16 stores share information. I mean it is your document so

17 you should know one way or the other.

18 A. So I would say that by integer that means everybody.

19 Whether you are third party or first party, what does it

20 matter? I do not understand your question.

21 Q. Do you agree that US Cybersecurity & Infrastructure

22 Security Agency document does not say anything about

23 whether third party app stores share information?

24 A. It does not need to. It talks about how the industry

25 works.

1 THE CHAIRMAN: Just answer the question. Is that the case,  
2 that it does not?

3 A. I mean, sorry -- thank you for the clarification.  
4 I would rather you put that document in front of me and  
5 I can take a look.

6 MR KENNELLY: {D2/609}. Just scroll through it, please. It  
7 talks about "information sharing is essential to  
8 furthering cybersecurity for the nation". Talks about  
9 the "importance of sharing information". CISA's role.  
10 Skip down, please. Next page, please. Next page,  
11 please. Next page, please. This is just to refresh  
12 your memory.

13 A. Okay.

14 Q. You will be re-examined on it if there is anything in  
15 there that helps you, but you do not see anything that  
16 talks about information sharing by third party app  
17 marketplaces do you? Does that jog your memory?

18 A. It does not specifically include or exclude anybody.

19 Q. In fact, there is a lack of alignment along vetting and  
20 mitigations. Could I bring you back to the National  
21 Council for Cybersecurity again, please. This is  
22 {D1/1273}. Do you recognise this document? Page  
23 {D1/1273/5}, please. If we zoom in on the box on the  
24 top left-hand corner, right-hand column:

25 "Moreover, there is limited evidence of coordination

1 and alignment between app stores on their vetting  
2 processes and mitigations against these  
3 vulnerabilities."

4 A. Okay.

5 Q. You are aware of the example given in Dr Rubin's report  
6 about Google banning copycat apps and they both remained  
7 on the Samsung Galaxy Store for several months. Does  
8 that ring a bell?

9 A. No, I mean, can you point me to the report?

10 Q. {C3/1/124}. Sorry, {C3/2/124.}. It is paragraph 239 of  
11 Dr Rubin's report. Second sentence:

12 "In 2023 a fake version of a popular messaging  
13 app ... was identified on the Google Play Store. The  
14 imposter app was embedded with trojan malware ...  
15 It remained available on Google Play Store for  
16 nine months ..."

17 If you skip down:

18 "However, even though Google took it down, both apps  
19 remained available on the Samsung Galaxy Store ... as  
20 of May 2024 ..."

21 So they had been removed, they had been removed by  
22 then but they remained in the Samsung Galaxy Store  
23 notwithstanding the fact that they had been taken down,  
24 even though the apps had been taken down by Google.

25 That suggests a failure to share information, does

- 1           it not, or a failure to act on information?
- 2       A.   So I do not recall what this imposter app is in terms of
- 3           the kind of action that it performs. My experience is
- 4           that if this is a major attack that information normally
- 5           is shared pretty quickly and action will be taken, but
- 6           otherwise I do not know, sometimes something can fall
- 7           through the crack I guess.
- 8       Q.   Now you say Apple could require third party marketplaces
- 9           to share the information, there could be a contractual
- 10          requirement for them to share information?
- 11      A.   Yes.
- 12      Q.   But for that to work the third party app marketplaces or
- 13          Apple would need to create the infrastructure required
- 14          to engage in that sort of realtime reporting, would they
- 15          not?
- 16      A.   Yes. I mean having a common website to upload that is
- 17          the starting point. It is easy.
- 18      Q.   They would have to create the infrastructure to review
- 19          and sift through all the information that it is sharing
- 20          because it goes in both directions, from Apple to the
- 21          third parties and third party marketplaces to Apple?
- 22      A.   Yes, but they already have their review process, do they
- 23          not? You just go and download the stuff and review
- 24          them.
- 25      Q.   Not all third party marketplaces have reviews and we do

- 1 not know anything about the quality of them?
- 2 A. But that is not the statement or assumption they have  
3 made. Even for counterfactual I say when you open up  
4 and take away the restrictions third party play stores  
5 they can review their apps just like Apple. So my  
6 assumption is they will have that same review process.
- 7 Q. Now, in this situation where information has been shared  
8 a malicious actor could pose as a third party app  
9 marketplace to obtain that information for illicit  
10 means, could they not?
- 11 A. That would not work in my industry group suggestion.  
12 You mean for you to be a third party marketplace you  
13 need to apply to say, hey guys, I am here. So again,  
14 some of these kind of checks is not 100% great but it  
15 works to mitigate a lot of would be bad behaviours.
- 16 Q. This contract that Apple would have with the third  
17 parties, it would need to be policed and enforced, would  
18 it not, the obligation to share information with Apple?
- 19 A. Yes, to me the principle of accountability transparency  
20 would go along way.
- 21 Q. How would Apple know if the third party marketplace is  
22 feeding it the information that Apple needs to ensure  
23 there are no malicious apps?
- 24 A. I think we went through this multiple ways. One is  
25 Apple already as iOS can log everything about how users

1 interact with the third party market place. The second  
2 thing is that if Apple is still not sure Apple can act  
3 as a user and go to this marketplace and find out what  
4 is going on.

5 Q. Dr Lee, iOS will not be logging every social engineering  
6 attack as they happen?

7 A. They could.

8 Q. Yes, but that is not the position on the DMA. It is not  
9 currently possible.

10 A. Technically it is possible.

11 Q. How would Apple know -- let's assume, as you are  
12 assuming that the third party app marketplace is  
13 providing information to Apple. How would Apple know if  
14 the third party is delaying the provision of that  
15 information?

16 A. Like I said Apple could go to these stores and download  
17 stuff and say, okay, now I did detect a malicious app  
18 and then you wait for a week or two for that marketplace  
19 report to go to you so you know there is a delay. Look,  
20 all these things are technically so feasible. It is  
21 about whether Apple wants to be or not or how it  
22 actually negotiate with industry group members.

23 Q. But let us assume that Apple needs information from  
24 a third party marketplace, that marketplace might have  
25 an incentive to hide information about malware that is

1 appearing in their systems to avoid Apple finding that  
2 its App Review is inadequate?

3 A. Then Apple can detect that immediately because they  
4 detected, hey, some iOS devices users downloaded this  
5 malicious app from that place and then you can find that  
6 marketplace, they say we do not have it.

7 Q. But Apple will not know it is suspicious until the  
8 problem arises?

9 A. Well, if the problem does not arise, then probably the  
10 malicious activity is not affecting the user yet.

11 Q. When the users are affected Apple will not know  
12 automatically. It needs to be told?

13 A. It depends on the malware. Like I said, if the malware  
14 ends up -- a lot of malicious apps and end up violating  
15 some kind of access control policy. Apple can catch  
16 that immediately, and also I think I said this  
17 throughout my reports, that Apple should and could  
18 actually use more malware detection and removing tools  
19 just like the macOS and I also notice that Mr Federighi  
20 said those are not the most advanced ... Just deploy  
21 even more advanced tools. What is stopping you?

22 Q. These are marketplaces. The developers distributing  
23 directly. They have no incentive to report their  
24 problems to Apple, do they?

25 A. Can you repeat that question again?

1 Q. We are talking about Apple needing information from the  
2 other sources that are distributing apps?

3 A. Right.

4 Q. The developer is distributing directly to users. They  
5 do not have an incentive to report problems. Many of  
6 them will not have an incentive to report their problems  
7 to Apple?

8 A. Again, it depends what information you need. Okay, so  
9 technically even if the developers does not specify what  
10 the app is doing you can still analyse the app and  
11 figure this out. That is what me as a malware analyst  
12 would do. The malware author never tells you what the  
13 malware is about. Finding the malware behaviour is  
14 a challenge that we face every day.

15 Q. So Apple needs to become like the user in realtime of  
16 every app downloaded from every source in this  
17 counterfactual?

18 A. That is the same thing what the app user is doing right  
19 now for App Store, what is the difference?

20 Q. Now, talking about the third party marketplaces and the  
21 information they have for their own App Review, they  
22 will have less information than Apple has for training  
23 their tools and human reviewers.

24 A. I am sorry?

25 Q. Third party app marketplaces will have less information.

1           They will have a smaller database to train their tools  
2           and human reviewers?

3           A. Again, I think I went through this. To me if I want to  
4           open up a third party app store to compete with Apple  
5           I would focus on some sectors like gaming, sports,  
6           entertainment instead of just compete in general.

7           Q. You talk about ex post facto. You say that Apple can  
8           pick up problems by sweeping after the downloads have  
9           taken place?

10          A. Yes.

11          Q. But again, that means that there will be a delay,  
12          I mean, inevitably Apple will not pick things up  
13          immediately. There will be a delay in the information  
14          reaching Apple?

15          A. Web sweeping is very fast. That is how Google, all  
16          these companies, view the database for searching. It is  
17          superfast.

18          Q. You saying here that Apple needs to do continual  
19          sweeping of every app that is downloaded continually?

20          A. You bet it, yes, and they can do it. We have been doing  
21          this for 20 years. People have been doing this web  
22          search for 20 years.

23          Q. You have not assessed how much that would cost in your  
24          report, have you?

25          A. Whatever. Apple has plenty of money to support it I bet

- 1           you.
- 2           Q. You have not described how that would be feasible in  
3           your report at all, have you?
- 4           A. To me anybody will tell you that is what anybody would  
5           expect a company can do.
- 6           Q. You say anybody, but you have not referred to any report  
7           or any study where anyone else is saying what you have  
8           just told the Tribunal?
- 9           A. You can ask any computer scientist. It is just a  
10          commonsense thing.
- 11          Q. Have you asked any other computer scientist?
- 12          A. Look, sorry, I was scanning the web in the mid 1990s.
- 13          THE CHAIRMAN: Dr Lee, I do not think you need to answer  
14          that question.
- 15          MR KENNELLY: Now we come to the last counterfactual where  
16          Apple applies full App Review to every app  
17          pre-distribution and that leaves open the possibility of  
18          malicious developers misleading Apple, okay.
- 19          A. Sorry, can you repeat that scenario again?
- 20          Q. A developer can submit a very basic app to Apple for App  
21          Review, with an accurate but basic information sheet, so  
22          there is no malware, complies with the guidelines. But  
23          on the developer or marketplace website the app is  
24          marketed as having lots of amazing features?
- 25          A. Mm-hm.

1 Q. So the person spends, say, £30 on it, on the website,  
2 downloads it on to iOS, discovers that it is very basic.  
3 They have been ripped off.

4 A. Yes.

5 Q. Apple's App Review is not going to spot that?

6 A. Yes, I mean, that is false advertisement. To me Apple  
7 could have done what I suggested right, they have  
8 a resource sheet that basically has information that the  
9 developer has sent to App Store when it do the  
10 notorisation, right. But then Apple can also, like  
11 I said, call the third party places that -- ah, you are  
12 showing the different screenshots. That is  
13 a discrepancy, so maybe they can catch that.

14 Q. So Apple has to proactively review how every developer  
15 is marketing itself continually on every other  
16 alternative source?

17 A. They could do that but then a better solution could be  
18 in the industry group as all the third party marketplace  
19 to make sure there is no such advertisement, meaning  
20 that app developers should not pose a bunch of  
21 screenshots that is different from the in store sheet.

22 Q. So you are hoping the industry group will make sure that  
23 malicious developers will behave them themselves?

24 A. I would say that is a requirement they should put in to  
25 stop and prevent the malicious developers, why not.

1 Q. Any user complaints about this scam are unlikely to be  
2 reported to Apple, are they? They are going to go to  
3 the developer or the third party marketplace first?

4 A. I do not know. I mean, I heard that most users would  
5 believe, hey, Apple owns everything and you come to  
6 Apple first. So I do not know.

7 Q. Similarly an app could be passed by App Review as  
8 a personal money manager. Very basic app, keep track of  
9 your spending, set up a login, make a list of your  
10 payments, they could be added up by the app. So very  
11 generic, no malware, passed by App Review.

12 The same problem, on the alternative marketplace  
13 or website the developer pretends to be a bank and not  
14 with this app is a banking app. The website says  
15 download it into your current details. The user  
16 downloads it, sees the very generic information sheet  
17 and then just the bank account details and they are gone  
18 to the bad actor. An App Review would not spot that,  
19 would it?

20 A. Okay, it is two things. If false advertisement we  
21 covered that, right, meaning that you can request third  
22 party Play Store to not allow false advertisement or you  
23 can call the third party marketplace to detect that.  
24 But if you are saying no, that is not about false  
25 advertisement, it is about bait and switch app

1           behaviour. In that case I am going to counter to say  
2           look, the notarisation process in EU is actually as good  
3           as the app process with regard to malicious behaviours.  
4           If the notarisation process had failed, then I do not  
5           believe the full Apple App Review will catch that  
6           either.

7           Q. But the difference is even in the current world if  
8           Apple's App Review misses it Apple is able to take down  
9           that app from its App Store immediately when a problem  
10          arises?

11          A. That is true but then, maybe like I said, the industry  
12          group can work out a standard as, hey, we detect  
13          a malicious app and you should block cancel everybody  
14          and everybody should take it down.

15          Q. So Apple has to rely on the intervention of the  
16          willingness of the app marketplace to remove these apps  
17          if Apple requests them to?

18          A. I do not see why that should not be a requirement.

19          Q. There may well be a delay in doing that?

20          A. Okay, so --

21          Q. Compared to Apple doing it directly and immediately  
22          itself?

23          A. So I do not know how long is the delay. No, I do not  
24          know.

25          Q. The longer the delay lasts though the longer the app is

- 1 available for iOS users?
- 2 A. We should not assume there is a delay that is so serious  
3 because, like I say, the industry group can also say,  
4 hey, this kind of alert should be in realtime. Could be  
5 acted upon in realtime. So I just -- these are very  
6 detailed implementation, yes.
- 7 Q. Because they are detailed and difficult a delay is very  
8 likely?
- 9 A. I do not think it is difficult. I mean, I think other  
10 industry have done this in securing national data, they  
11 have done this.
- 12 Q. But you accept if there is a delay the longer it lasts,  
13 the more potential there is of harm to the user?
- 14 A. Yes, sure, but you could say some of the malicious apps  
15 on App Store is not immediate picked up either. There  
16 is some delay. So I do not think --
- 17 Q. You are saying --
- 18 A. -- require or expect a perfect process.
- 19 Q. So I must say, it is just implausible that there will be  
20 no greater delay when Apple is relying on third parties  
21 to decide whether to take it down compared to Apple  
22 deciding it itself?
- 23 A. So it is not always guaranteed that when you have  
24 industry groups it is always more delayed than Apple  
25 itself. I just do not think you can categorically say

1           that either.

2       Q. No. So overall you are positing a counterfactual world  
3       where we have centralised verification and certification  
4       at the beginning of the process but Apple checks  
5       identities and decides which developers get to  
6       distribute. Centralised App Review of every single app  
7       before distribution?

8       A. You mean notarisation?

9       Q. Notarisation.

10      A. Yes.

11      Q. Then decentralised distribution in the middle of the  
12      process?

13      A. Mmm.

14      Q. Apple has no control over how the apps are being  
15      presented on alternative platforms apart from its  
16      requests that people behave. It is no longer the  
17      central repository for information and data on how those  
18      apps are operating, subject to the technical changes  
19      that you mention?

20      A. So all the things you describe so far is what has been  
21      practiced in EU but that is not how I would recommend in  
22      the counterfactual. In the counterfactual I say we  
23      should have an industry group, that better organise,  
24      better regulate, better incentivise, whatever, better  
25      help each other.

1 Q. So at the end of the process you have centralised  
2 enforcement by this industry group which decides whether  
3 malicious actors are taken down or not?

4 A. I would not call it centralised. But it is a group  
5 thing.

6 Q. So actually you do not envisage any enforcement by Apple  
7 on its own at the end of this process?

8 A. What do you mean?

9 Q. Well, do you envisage in your counterfactual the  
10 possibility that Apple itself will decide whether to  
11 take down what it decides are malicious apps or not?

12 A. Yes, sure, if it sees an app in an app store of course  
13 it will do that.

14 Q. In this scenario the developers like Google, Google Play  
15 Store will know that Apple will be verifying every iOS  
16 identity, perform an ex ante review, checking if the  
17 apps are code signed, policing the post-distribution  
18 world for signals, and potentially enforcing as well,  
19 yes?

20 A. I do not know why you throw in Android. It is a bit of  
21 a confused --

22 Q. The Google Play Store would be potentially -- They would  
23 not have to carry out any of these services itself?

24 A. But I do not know why Google Play Store is in the  
25 picture. We have been talking about iOS, right?

1 Q. But in the counterfactual the Google Play Store could be  
2 on iOS and it would know that it would not have to do  
3 any of these things that Apple is doing in your  
4 counterfactual?

5 A. Okay, if Google Play Store offers iOS app I would say  
6 they are part of the industry group, they should conform  
7 the same standard. They are no different.

8 Q. But in your counterfactual here Apple is doing all of  
9 these things except the actual distribution in the  
10 middle of the process, correct?

11 A. What do you mean?

12 THE CHAIRMAN: I think, Mr Kennelly, you put the point. You  
13 are not going to get a lot further.

14 MR KENNELLY: So the extent that Apple is doing all these  
15 things it will be entitled to charge third party app  
16 marketplaces for these benefits?

17 A. That is beyond me. I do not know.

18 Q. Just to be clear, you are not aware of any company in  
19 the world that has set up this kind of security  
20 architecture, have you?

21 A. Okay, so industry group I know plenty. Like I said, the  
22 ad tech industry that Google is actually part of, they  
23 have industry group, they do talk about some standard  
24 stuff.

25 Q. But they do not decide if apps get taken off Android or

- 1 not. It is Google's decision?
- 2 A. I am not sure that is the case. I mean, if you are a  
3 device manufacturer you probably can do things too.
- 4 Q. So this is a security strategy that has never been  
5 implemented or tested in the real world?
- 6 A. You mean industry group?
- 7 Q. No, the whole thing that you described actually has not  
8 been tested or implemented in the real world?
- 9 A. What do you mean the real thing?
- 10 Q. The idea that Apple is running on a continual basis all  
11 downloaded apps distributed by everyone on iOS as if it  
12 were a user and subjects the removal of apps to external  
13 control?
- 14 A. So Google Play, like I said, actually scan every day on  
15 every device all the apps that have been downloaded and  
16 also scan the web to collect as much information as  
17 possible. So I think Google Play is doing something  
18 very close to what I just described.
- 19 Q. You say that the Tribunal should find that this  
20 hypothetical strategy is as effective or better even  
21 than Apple's current set up?
- 22 A. I did not say it has to be better but I do not think it  
23 is worse. It could be -- like I said, it could be even  
24 beneficial. My -- I think I said this in my report.  
25 I say that if a third party app store is specialised, as

1 in gaming, it actually takes the workload off Apple's  
2 App Store, so Apple's App Store actually can spend more  
3 with each app.

4 So my point is that technically by having this open  
5 app store kind of a model where there is a big player,  
6 let us Apple, and the other smaller players specialise  
7 in their own domain, then actually they could do  
8 a better job.

9 Q. But, Dr Lee, you are wrong because in this situation  
10 Apple would have less information and data points?

11 A. But I think we went --

12 Q. Timely information data points by which to identify  
13 problematic apps?

14 A. But I think we went through this already. First of all,  
15 iOS can detect which app you are downloading and whether  
16 this app is doing something bad.

17 Second of all, like I said, if Apple still find that  
18 is, I do not know, less time it can also actively scan  
19 all the marketplaces. So none of these to me is just no  
20 technical challenge that would prevent Apple from taking  
21 on information it needs.

22 Q. Final topic, sir. I am now on payment restrictions. I  
23 will move through quickly.

24 THE CHAIRMAN: How long will you be?

25 MR KENNELLY: Less than ten minutes.

1 THE CHAIRMAN: Yes, thank you.

2 MR KENNELLY: So now we are on payment providers and even  
3 taking into account the possibility that a particular  
4 payment provider might store users' payment information  
5 in their own systems, by itself that means iOS device  
6 users will be entering their payment details more often  
7 than they do currently.

8 A. Can you point me to my report where I discuss this?

9 Q. No, Dr Lee, I am asking you a very basic question.

10 A. Okay, so can you put the question again.

11 Q. If there are different payment providers storing payment  
12 information iOS users might well enter in payment  
13 details more often to use these payment providers?

14 A. It is possible, yes.

15 Q. Each time they enter their payment information into some  
16 kind of digital checkout they create a new opportunity,  
17 just opportunity, for attackers to get hold of that  
18 information?

19 A. Yes, in principle, I mean, but if I am a sophisticated  
20 attacker, I could also attack Apple's whatever storage  
21 of your payment information too.

22 Q. If a given payment provider does offer the option of  
23 saving payment option for use in future transactions  
24 that means there is another third party company which is  
25 storing their payment details as opposed to one

- 1           currently?
- 2       A. Yes, but like I say in my report, it is no different  
3           from how people buy things online through websites.  
4           What is the difference?
- 5       Q. That third party database storing information might  
6           itself be a target for attackers?
- 7       A. Yes, that is like Apple can also be attacked.
- 8       Q. So in this counterfactual attackers will have greater  
9           opportunities to acquire users' payment details than  
10          they currently do, simply because there are more  
11          targets?
- 12      A. I am not sure because some of the examples I gave, let  
13          us try, they are very big. I think they probably have  
14          as good security as Apple.
- 15      Q. Let us look at those prioritisation of security issues.
- 16      A. Okay.
- 17      Q. Let us assume there is a world where developers are able  
18          to work with different payment providers. We are likely  
19          to see those different payment providers spending  
20          different amounts of money on security?
- 21      A. Okay.
- 22      Q. Some of them just will not be earning the same profits  
23          as the others to invest in their systems?
- 24      A. Okay.
- 25      Q. Others might choose a different trade off. They may

1           prioritise profits over security and offer a less gold  
2           star product?

3       A.   Okay, so I mean, in your hypothetical situation I would  
4           tell you that any payment system that behaves like what  
5           you describe would go down in no time.

6       Q.   Some developers may deliberately choose their cheaper  
7           payment provider?

8       A.   The user will avoid them. First of all, if it got into  
9           trouble with stolen credit cards, stolen cheque, the  
10          acquirer bank normally cover that immediately. So as  
11          the financial institution or payment system you know  
12          most of time you cover the loss. If you refuse you go  
13          down right away. Nobody can use it. That is common  
14          sense.

15      Q.   But again, users are not able to make reliable judgments  
16          about the relevant security or otherwise of particular  
17          payment systems?

18      A.   The user has been buying things online all the time  
19          already so they already know some reputable payment  
20          systems. They know what to avoid. So to me, let us not  
21          assume the users are that stupid. I am sorry for my  
22          language. I am sorry. But to me we are being very  
23          arrogant here to say, hey, user data is dumb, they would  
24          make all this mistake. They would go on the web and  
25          they buy things.

1 Q. But if the developer is itself a malicious attacker that  
2 developer might even purport to process payments itself  
3 to get access to the customer's payment details?

4 A. So my question is how does that malicious developer get  
5 on the App Store and then get away with it? Because,  
6 like I said, I insist that when you open up you should  
7 still enforce developer ID, verification and app  
8 signing. So committing a financial fraud is a huge  
9 deal. Most ID would be reported to FBI. So I mean,  
10 I would not -- I do not want to think that kind of  
11 possibility.

12 Q. Dr Lee, there are social engineering attacks that do  
13 exactly that. Even on iOS currently that have attempted  
14 to get payment details, malicious actors getting payment  
15 details directly from users, do you accept that, through  
16 social engineering?

17 A. Yes, so social engineering is a little bit more  
18 complicated, right, meaning that you essentially accept  
19 false advertisement.

20 Q. In terms of information and fragmentation you accept  
21 that the more information one has about different  
22 transactions the better one's systems can become at  
23 identifying fraudulent or potentially fraudulent  
24 transactions?

25 A. Yes, in principle the more data the better, yes, sure.

1 Q. One of the requirements of distributing an app through  
2 the App Store is any payments for any app purchases are  
3 facilitated through Apple's commerce engine so Apple  
4 obtains all the information and that means it gets more  
5 information than it would in the counterfactual where  
6 third party systems will be processing the payments?

7 A. That is a possible, yes.

8 Q. That means Apple systems will be less effective at  
9 identifying fraud relative to the world where it was  
10 getting all of the transaction data. It will have fewer  
11 data points?

12 A. Yes, that is possible, yes.

13 Q. In a counterfactual world where transaction data has  
14 been routed through a third party payment provider and  
15 it sees a problem with the payment that third party will  
16 have less background knowledge of the app itself  
17 because -- less than Apple, because Apple will have done  
18 the App Review?

19 A. Yes, so I think I covered this in my report. First of  
20 all, all apps would be reviewed the same way, whether  
21 you use Apple's payment system or a third party payment  
22 system so the obvious bad things can be reviewed and  
23 detected.

24 The second thing is that I would bet that most users  
25 or honest brokers would use a trusted reputable payment

1 system and those systems have a long history of  
2 detecting frauds. They have all the data as well.

3 Q. The third party payment provider has no means of  
4 removing the app from the App Store, the ones identified  
5 as problematic?

6 A. But look, if our payment system, I know that this app  
7 caused a fraud and I pay back to the users. Guess what  
8 I am going to do. I am going to tell Apple.

9 Q. There is no way that third party payment provider can  
10 suspend the customer account, the one that is on the  
11 Apple's site?

12 A. What do you mean suspend the customer account? What do  
13 you mean?

14 Q. If the fraudulent person is the app user, the iOS user,  
15 he cannot stop that person operating on iOS?

16 A. You mean the --

17 Q. The customer. It could be a fake customer.

18 A. A fake customer?

19 Q. A fraudulent customer.

20 A. But like I said, the payment system when they have  
21 financial loss they have incentive to call Apple.

22 Q. But Apple currently can do all these things immediately  
23 because of its position as manufacturer, developer and  
24 operator of the App Store, developer of the operation  
25 systems?

1 A. Yes, sure, if you have the monopoly of everything, yes,  
2 sure, everything goes through you.

3 Q. So for those reasons there is a security benefit to iOS  
4 device users in Apple operating a centralised system for  
5 distribution and payments?

6 A. Yes, but my position is the same benefit can be borne  
7 out when you open up and let a third party payment  
8 system to help.

9 MR KENNELLY: Thank you, Dr Lee, I have no further  
10 questions.

11 THE CHAIRMAN: Thank you, Mr Kennelly. Well done. Finished  
12 just on time.

13 Re-examination by MR KENNEDY

14 MR KENNEDY: Just four questions, sir.

15 Dr Lee, you were asked some questions about  
16 manufacturers of Android devices and updates to the  
17 Android OS. Do you recall that?

18 Q. Updates to the Android OS security practice. Do you  
19 recall that?

20 A. Yes.

21 Q. Can you go to {D1/518/1}. Dr Lee, you see this is an  
22 email from Craig Federighi. Do you know who that is?

23 A. Yes.

24 Q. To Tim Cook and Philip Schiller who are all Apple  
25 employees, okay. It is dated 16 March 2018. If we

1           could scroll half the way down you will see an email  
2           from Mr Cook from the day before. If we scroll down  
3           a bit. You will see that it appears to be a copy and  
4           paste of an article of 9 to 5 Mac. Can I ask you to  
5           just read the first paragraph there starting "Android's  
6           head", please. Let me know when you have finished. Go  
7           to page {D1/518/2}. We are going to pick it up about  
8           halfway down. Can I ask you to read from the words "He  
9           acknowledges the big problem" and then go over the page  
10          when you are ready and ask the operator to go over the  
11          page.

12          A. Okay. {D1/518/3}.

13          Q. Just read until you get to the break in the paragraph,  
14          please. (Pause). Could we just go back to page 1.

15          Could I ask you to read Mr Federighi's email to Mr Cook.

16          A. Yes. (Pause). Okay.

17          Q. Do you have any comment on that document, Dr Lee?

18          A. I am sorry, what?

19          Q. Do you have any comment on that document?

20          A. So I mean, it is not surprising the statement that  
21          Android are secure as not more than secure than iOS.  
22          I think in my second report I cited recent industry  
23          report in terms of the bounty, the bug bounty for  
24          Android now actually pays more than iOS bounty, meaning  
25          that it is harder to find security tags on Android than

1           iOS. So that is very recent.

2           Second of all, I think I mentioned a couple of times  
3 throughout my testimony today that Google Play really  
4 went a long way in terms of scanning what apps to  
5 download and then try to detect and enimise(?) those  
6 apps. So there are multiple advances in Android that  
7 makes it more secure.

8           Q. Thank you. Could we go to {D1/1,745.1}. You were shown  
9 this document by Mr Kennelly. Could we just zoom in  
10 just to the top part of this and could I ask you to read  
11 the second sentence which begins "Website operators".  
12 Do you see that?

13          A. Mm-hm. (Pause).

14          Q. You will see at the end of this sentence there is  
15 a footnote. Can we go to the end of the document and we  
16 will see what the footnote is.

17          A. Okay. Can I see the footnote?

18          Q. The document that appears behind that hyperlink is at  
19 {D2/645.1}. Dr Lee, this is a web page in Apple's  
20 support website. Could I just ask you to read the  
21 paragraph under the heading "About certificates",  
22 please?

23          A. Okay. (Pause).

24          Q. Could we go to page 11, please. {D2/645.1/11}, please.  
25 Could we zoom in. Just scroll down a bit so we have the

1 second entry. Can I ask you to scan, Dr Lee, from the  
2 second entry over the page under 12 and on to 13.

3 A. Okay. {D2/645.1/1-13}.

4 Q. Then over on to page 14 and could I ask you to start  
5 with the second entry and again scan down 14 and over to  
6 the first entry of 15. {D2/645.1/14-15}. Then could we  
7 go to page {D2/645.1/33} and could I ask you to look at  
8 the second entry.

9 A. Yes.

10 Q. Again, do you have any comment on that document?

11 A. Yes, so this tells you that I think that DigiCert,  
12 Entrust and VeriSign, they are all trusted by Apple for  
13 the web-based Apple apps.

14 Q. Thank you, Dr Lee.

15 THE CHAIRMAN: I am not sure I understand that answer.

16 Would you mind just explaining that again, Dr Lee?

17 A. So basically these are the new certificates that are  
18 trusted by Apple which means that certificates that are  
19 issued or signed by these authorities Apple would allow  
20 it, would basically would trust and then allow the  
21 browser to visit those websites and then -- so when you  
22 visit a website there is an indication to say, hey, you  
23 are visiting Google. How do you know? There is  
24 a verification of what signature you have as Google. So  
25 that that key for you to claim as Google has to be

1           issued by a certificate of authority. What it is saying  
2           here is that Apple trust DigiCert, Entrust and VeriSign  
3           to sign Google's key to say, yes, that is Google.

4   THE CHAIRMAN: This is the link back to the previous  
5           document which was the announcement that certain  
6           certificates would not be accepted. Can you explain the  
7           connection between the two?

8   A. Yes, so the connection is basically saying, I think  
9           Symantec say now you basically visit this website to  
10          know which certificate is being trusted.

11   THE CHAIRMAN: So Apple were saying we are not going to  
12          trust some, in the first document we saw, which was --

13   MR KENNEDY: Sir, if it would help we can go back to  
14          {D1/1745.1} and it is the second sentence, sir, I think  
15          that explains the alternatives. Perhaps just reread  
16          "website operators," until the end of the sentence.  
17          That might help.

18   THE CHAIRMAN: Yes, I see.

19   A. Yes.

20   THE CHAIRMAN: Yes, I understand.

21   A. So basically the document that we just saw lists all the  
22          certificate authorities trusted by Apple and those  
23          include DigiCert, Entrust and VeriSign which I included  
24          those in my report.

25   THE CHAIRMAN: I understand, thank you.

1 MR KENNEDY: Can we go to today's transcript, 171, line 25.

2 Dr Lee, could I ask you to read from the question which  
3 starts "Another type of information" and could you read  
4 down to line 15 on the next page.

5 A. Okay. (Pause). Yes, there are a lot of typos, sorry.

6 Q. Then could we pick it up at line 24 of 172. Just scroll  
7 down and then could I ask you, you will see the  
8 question:

9 "Yes, but to the extent which problems arise."

10 Could I ask you to read that question down to your  
11 answer which ends at line 6 on page 173. (Pause).

12 A. So where shall I start?

13 Q. Stop at line 6?

14 A. Okay.

15 Q. I think some confusion arose between you and Mr Kennelly  
16 about the information that could be provided by iOS in  
17 the circumstances of the discussion and information that  
18 might need to provided by a third party app store.

19 I was just wondering could you explain to the Tribunal  
20 what information could be provided by iOS back to Apple  
21 in the circumstances under discussion, please?

22 A. Yes, so I think iOS actually can monitor what apps and  
23 from which source this is being downloaded. So if there  
24 is an app which has been downloaded from a third party  
25 app store iOS knows that. It can actually report back

1 to Apple and also iOS has on device and run time  
2 protection so if the app behaves badly, it violates the  
3 security policy that Apple is monitoring including sand  
4 box or in the future some additional tools Apple can  
5 know that and then report it to Apple as well, so that  
6 is on iOS.

7 On the marketplace then of course that information  
8 about how the app has been advertised and so on and so  
9 forth. For that kind of information Apple can through  
10 the industry group request all the marketplaces which  
11 shared information, but absent from that Apple can also  
12 scan or pretend to be user to download that information  
13 and find out.

14 Q. Final question, Dr Lee. Can we go to {D2/689/1},  
15 please. {D2/609}. You were shown this document earlier  
16 Dr Lee; do you recall that?

17 A. Mm-hm.

18 Q. Could we just zoom in on the bottom paragraph, "CISA's  
19 role", and can I ask you to read the first sentence:

20 "As the lead Federal department" until the word  
21 "programmes".

22 A. Yes.

23 Q. Do you have any comment on that, Dr Lee?

24 A. Yes. Actually I am I have been to, I have been  
25 throughout my career been funded by the Federal

1 Government of US. I remember on a panel some people in  
2 the audience say, information sharing and the panel  
3 actually consisted of a bunch of executives from leading  
4 security companies. They say, yes, we are actually  
5 doing information sharing. Much more than you actually  
6 realise. We do information sharing every day. Also you  
7 work for, let us say, the Homeland Security, one of the  
8 requirements that we share information. Like I said,  
9 I work for -- my contract with DHS, ten years we analyse  
10 half a million samples, a sample every day. What we do,  
11 we check the behaviours and then we share them with all  
12 parties that DHS had approved. Then one time I went to  
13 Israel for security meeting and people came up and  
14 thanked me for that.

15 So information sharing really happens much, much  
16 more than people realise but anyway, yes.

17 MR KENNEDY: Thank you, Dr Lee. No further questions from  
18 me, sir, thank you.

19 Questions by THE TRIBUNAL

20 DR BISHOP: Just one really tiny point, I hope, Mr Kennedy,  
21 I was struck with that email from Mr Federighi that you  
22 put to Professor Lee. There is a sentence in there, the  
23 third sentence if memory serves which said we will see  
24 if the price that Android vulnerability rises to, and  
25 then something about Apple.

1 MR KENNEDY: Can we have it up, {D1/518}. That may assist.

2 DR BISHOP: I have no idea what he was talking about. Do  
3 you know?

4 MR KENNEDY: I am loath to give evidence from the Bar.

5 A. So I would give you some anecdotal -- first of all,  
6 I will be careful strictly, not confidential, but some  
7 of my team member students who were involved in the  
8 Jekyll app, later on in their career they became  
9 essentially a bug finder. Some of them actually make  
10 seven figures out of Apple. I am not joking. They find  
11 bugs of iOS and Apple would pay them. One of them, the  
12 lead author of Jekyll, make more than me, put it this  
13 way.

14 So basically right now the report cited in my second  
15 report is that the price, the price tag for Android bug  
16 is actually higher or higher than iOS. That is the  
17 point, as evidence, another evidence that Android is  
18 more secure than we think.

19 DR BISHOP: Right.

20 MR KENNELLY: You mentioned my name, Dr Bishop, did you have  
21 anything for me?

22 DR BISHOP: It is.

23 MR KENNELLY: It is the bounty programme.

24 DR BISHOP: In that --

25 MR KENNELLY: It is the bounty programme. It is what people

1           pay to show Apple or Android the vulnerability that they  
2           discover.

3       THE CHAIRMAN: Thank you. Anything arising from that?

4       A. Also they make some money on the side which makes me  
5           very envious.

6       THE CHAIRMAN: Okay.

7       DR BISHOP: That is fine.

8       THE CHAIRMAN: Thank you very much. Dr Lee, that concludes  
9           your evidence. Thank you very much and you are released  
10          from the witness box.

11      A. Thank you. May I add I stand by everything I said.

12      THE CHAIRMAN: You are finished, thank you. You can go now  
13          thank you very much.

14                So tomorrow we are going to be seeing  
15                Professor Rubin; is that right?

16      MR KENNELLY: That is correct, sir.

17      THE CHAIRMAN: Just in terms of getting a sense of how the  
18          rest of the week looks. One of the things that did  
19          arise earlier on at the timetable discussions is whether  
20          we had enough time this week and particularly there is  
21          enough time for the accounting experts. Just to help  
22          you a bit, we can start at 10.30 on Thursday but what  
23          I would like to know is whether -- the current  
24          configuration I think has the class representative's  
25          accounting expert in the afternoon of Wednesday and then

1 a day of -- so it is Mr Dudney and then a day of  
2 Dr Barnes on Thursday. I do not know if that is how you  
3 are thinking about it and I am not asking you to tell me  
4 the answer now, but it would be quite helpful if as  
5 counsel teams you could confer and make sure you are  
6 happy with the way the rest of the week works because  
7 basically we have to make it work. So one way or  
8 another you will need to find a way to get through  
9 everything you need to get through by Thursday night.  
10 There will be of course some accommodation for extra  
11 time but, as you will have picked up, particularly given  
12 the burden on the transcriber, there is only so much we  
13 can do for that.

14 So it would be quite helpful if we could know  
15 perhaps tomorrow morning just how tight it looks and  
16 where we think the pinch points are.

17 MR KENNELLY: Indeed, sir. I will speak to my team and we  
18 will liaise by tomorrow morning, fully aware of the  
19 difficulties on the Tribunal and on the transcriber.

20 THE CHAIRMAN: That is very helpful, thank you. Otherwise  
21 I do not think we have any particular constraints apart  
22 from I could not start early on Thursday morning. So if  
23 we do need to find a bit of time we can look for that  
24 but it will be subject to obvious limitations.

25 MR KENNEDY: Indeed, and I must just again thank the

1 Tribunal and the transcriber in particular for sitting  
2 on extended hours for the purpose of my  
3 cross-examination. It is of great assistance to me,  
4 thank you.

5 THE CHAIRMAN: Thank you very much. So we will start at --

6 MR KENNEDY: Did you say 10.30 on Thursday?

7 THE CHAIRMAN: I can start at 10.30. But I cannot start  
8 prior to that and if you wanted to have a --

9 MR KENNEDY: I do not think there will be any difficulties.

10 I do not envisage being longer than the appointed day  
11 and a half with Professor Rubin and I think a day and  
12 a half with the accountants.

13 THE CHAIRMAN: I seem to recall there being some dispute  
14 about there being a fair allocation.

15 MR KENNELLY: There was some dispute and that is what I need  
16 to come back on.

17 THE CHAIRMAN: Between the two of you collectively you need  
18 to work out how it is going to happen and it would be  
19 helpful to know that tomorrow morning so I can hold you  
20 to account.

21 MR KENNEDY: Understood, thank you.

22 Good, okay, 10.30 tomorrow morning.

23 (5.00 pm)

24 (The hearing adjourned until Tuesday, 28 January at  
25 10.30 am)

INDEX

1  
2 DR WENKE LEE (continued) .....1  
3 Cross-examination by MR KENNELLY (continued) .....1  
4 Re-examination by MR KENNEDY .....215  
5 Questions by THE TRIBUNAL .....222  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

1

2