IN THE COMPETITION APPEAL TRIBUNAL

Case No: 1403/7/7/21

Salisbury Square House
8 Salisbury Square
London EC4Y 8AP

Tuesday 28th 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 AN 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

Tuesday, 28 January 2025

(10.30 am)

Housekeeping

MR KENNEDY: Sir, we said we would come back to you on the timetable, so we start there.

THE CHAIRMAN: Yes.

MR KENNEDY: The position I have discussed with Mr Kennelly, so this is agreed, I hope to be finished with Professor Rubin before lunch tomorrow but we will see how we get on, and Apple expects to finish Mr Dudney on Wednesday.

THE CHAIRMAN: Okay, so Mr Dudney is only going to take an afternoon then, that is the plan?

MR KENNEDY: Potentially there is a bit more if I finish early.

THE CHAIRMAN: Yes, exactly. Yes, I think you do need to finish by lunchtime.

MR KENNEDY: There is no question I will not finish by lunchtime. I am hoping to finish a little bit earlier.

THE CHAIRMAN: In which case, you can give Mr Kennelly a bit of time back with Mr Dudney.

MR KENNEDY: Yes, exactly. Mr Piccinin will be the one who is dealing with Mr Dudney.

THE CHAIRMAN: Yes, quite.

MR KENNEDY: Dr Barnes will be available on Wednesday in

case Mr Dudney is finished early.

You have indicated, sir, that on Thursday you can start at 10.30, and the parties are keen to make use of that additional hour, and in the event that Mr Dudney runs over, it has been agreed that Apple take no more than 30 minutes of the additional hour on the Thursday.

I appreciate we are jumping back and forth between early and late.

THE CHAIRMAN: Yes, I am catching up. I see. So if Mr Dudney, for any reason Mr Piccinin needs more than an afternoon, possibly we could sit a little bit later tomorrow afternoon as well to help with that, but there is a bit of run-off time on Thursday morning, because I suppose there is a question as to whether you do need a whole day with Dr Barnes. Is that your expectation at the moment?

MR KENNEDY: The time estimate for Mr Ward and Mr Armitage is at least three-quarters of a day. That is what I am told, sir.

THE CHAIRMAN: Okay, that all works then, does it not?

MR KENNEDY: That all works, and that is the security and accountancy finished by the end of Thursday, as you indicated, sir, so I think we are in good shape.

THE CHAIRMAN: Good. Well, that is very helpful.

Thank you.

MR KENNEDY: I think the only other piece of housekeeping is the Tribunal should have received an errata sheet from Professor Rubin.

THE CHAIRMAN: Yes, we did.

MR KENNEDY: It has been agreed that will not be dealt with in chief, just due to its length, sir. Hopefully you have received a copy; I received a copy this morning at 8.30, I have not had a chance entirely to digest it but will endeavour to do so in the breaks, to make sure I can sweep up anything that arises out of it, but just making sure it is on your radar, sir.

THE CHAIRMAN: Yes, I have seen that. So if it is not going to be dealt with in chief, how will it be dealt with?

MR KENNELLY: It will be dealt with in chief in the sense that it will be confirmed by Dr Rubin and he will confirm that it is his signature, so his evidence will be sworn subject to these corrections which he will also swear to, so it will be introduced in that way.

When Dr Rubin asked for these corrections to be made overnight, and I saw there were seven textual corrections and 11 cross-reference corrections, it seemed a more sensible way to do it.

THE CHAIRMAN: Yes, it is very helpful to do it that way. So is the point that you have not seen them, so you are just reserving your position on them?

MR KENNEDY: I am just reserving my position, sir, exactly.
THE CHAIRMAN: So you are not objecting to them going into the record but you may have things to say about them.
MR KENNEDY: Yes, and that may not be until tomorrow, so there is a risk I will have to go back over material I have dealt with today because I have not had a chance to digest the corrections, sir. I hope that is not the case. I have done my best to look at them quickly this morning.
THE CHAIRMAN: I have to say, looking at them, it was not obvious to me there was going to be a problem, but obviously you should have time to look at them properly.
Good, thank you.
MR KENNELLY: So Apple calls Dr Aviel Rubin.
PROFESSOR AVIEL RUBIN (called)
THE CHAIRMAN: Can we swear Dr Rubin, please.
PROFESSOR AVIEL RUBIN (affirmed)
Examination-in-chief by MR KENNELLY
MR KENNELLY: Dr Rubin, you should have a hard copy file containing your reports and I will also call for them to be brought up on the screen.
For the screen, can we have {C3/2/1}, please. Thank you.
Do you have a hard copy of that as well?
A. I do.

Q. Can you confirm this is your first report in these proceedings?
A. Yes.
Q. Could you turn to page {C3/2/176}, please.
A. Okay.
Q. Is that your signature?
A. Yes, it is.
Q. Could you now be shown, please, your second report, {C3/6/1}.
A. I have that.
Q. Is this your second report in these proceedings?
A. Yes, it is.
Q. Could you turn now to page {C3/6/115}.
A. Okay.
Q. Is that your signature?
A. Yes, it is.
Q. Could you now go to -- could you be shown {C3/10/1} and you should have a hard copy of the corrections you wish to make. Is this the list of corrections you wish to make?
A. Yes, it is.
Q. Could you turn, please, to page {C3/10/5}. Is that your signature?
A. Yes, just on mine it is on page 4, but, yes.
Q. Can you confirm that with these corrections these

reports set out your expert opinion?

A. Yes.

Q. Insofar as the facts set out in these reports are within your own knowledge, that they are true?

A. Yes.

MR KENNELLY: Thank you, Dr Rubin. My learned friend Mr Kennedy has some questions for you.

Cross-examination by MR KENNEDY

MR KENNEDY: Good morning, Professor Rubin. I am going to be asking you some questions on behalf of the Class Representative.

A. Okay, good morning.

Q. You should have two bundles in front of you. You should have a black lever arch file which should contain your first report, your second report and the joint experts' statement. Do you have that?

A. I do.

Q. Then you should have a white file which should have 60-something tabs in it, 66 tabs in it?

A. Yes.

Q. Got that? Those are the documents that I will be taking you to in the course of cross-examination. There is only a limited amount of confidential material in those documents but I will indicate to you when something has been marked as confidential by Apple and I will ask you

to read it. I will not read it out and I would ask you likewise not to read it out. It may be that tomorrow morning we have a short session in private where there is a document that I would like to discuss with you which is entirely confidential, and I think we will be inhibited in our ability to discuss it if we do not go into private, but we will cross that bridge when we come to it.

A. Sounds good.

Q. I want to start, Professor, with your previous work for Apple. You acted as an expert for Apple in Grace v Apple in 2018, is that correct?

A. I do not remember the year but I was on that case.

Q. You acted as an expert for Apple in Epic v Apple Inc in the United States, yes?

A. Yes.

Q. Your firm also provided technical litigation consultancy services to Apple in connection with those proceedings, yes?

A. Yes.

Q. You acted as an expert for Apple in Epic v Apple Inc in Australia, yes?

A. Yes.

Q. Have you acted for Apple as an expert in any other legal or regulatory proceedings?

A. I believe there was a patent case that I was working on for Apple, but I do not think that case even reached the point of submitting an expert report, so I do not recall any others.

Q. So it is four or five times that you have acted for Apple as an expert, yes?

A. This is the fourth, I think.

Q. Plus the patent case that did not go to trial.

Can we pick up your first report, Professor Rubin, at paragraph 10, that is {C3/2/6}. You see it is at the bottom of the page. First report, {C3/2/6}.

A. Sorry, I had the wrong report. Yes.

Q. You see you say:

"In forming my opinion, I have also relied upon, in addition to my knowledge and experience noted above, the documents and materials cited here in and listed in appendix B to this report. These documents and materials include relevant academic literature, witness statements from Apple employees, Apple internal documents produced in and provided to me in this matter, and publicly available evidence."

Yes?

A. Right.

Q. Can we go to appendix B of that report which is {C3/2/200}, so page 200 for you.

A. I am there.
Q. You will see the first heading Is "Pleadings, Witness Statements and Exhibits", yes?
A. Yes.
Q. You refer to Mr Schiller's statement, yes?
A. Yes.
Q. Also Mr Federighi's statement, yes?
A. Yes.
Q. Did you have regard to the evidence of any other Apple employee in preparing your first report?
A. I do not believe so.
Q. But in preparing for the Epic proceedings in the United States, you had discussions with Mr Kosmynka and Mr Friedman, yes?
A. I remember speaking with Mr Kosmynka, and I may have spoken with Mr Friedman, I do not remember for sure.
Q. It came up in the Australian proceedings, Professor Rubin. So if we pick up the white bundle and it is tab 1. For the EPE, it is {G2/43/10}. If you look for page 10 on the bottom right-hand side you should be able to find it. Do you see that?
A. Yes.
Q. If we pick it up at line 5, you see -- or pick it up at line 0, actually:
"... you ... engaged in extensive preparation for

the proceedings between Epic and Apple in the United States?"

Then the question is:

"And that preparation included conducting interviews with Apple employees, including Mr Kosmynka, the head of App Review at Apple; and Mr Friedman, the fraud engineer ..."

Then you see your answer:

"Yes."

Does that refresh your memory in speaking with Mr Friedman?

A. At the time I must have remembered that I did, so I probably did.

Q. You spoke to Mr Kosmynka on two occasions; is that correct?

A. Yes.

Q. You did not make any record of those conversations, is that correct?

A. I do not remember making any record.

Q. You spoke to other Apple engineers, but what you said in the Australian proceedings is that you did not recall their names; does that sound right?

A. Possibly. I do not remember.

Q. Keep tab 1 open and we will have a quick look again at the transcript. It is page 11, this time. {G2/43/11}.

You see right at the top:

"And you spoke with various Apple engineers in the process of preparing for the US proceedings? ...

"And who were they? -- I don't remember."

Do you see that?

A. Yes.

Q. The information you acquired through those conversations with Apple employees formed part of the basis of the opinions you expressed in the United States Epic proceedings, yes?

A. Yes.

Q. You expressed the same opinion in the Australian Epic proceedings, yes?

A. There was a substantial overlap in the opinions that I expressed in those two cases.

Q. There was a substantial overlap between the opinions you gave in the Australian Epic proceedings and the opinions you have given in these proceedings?

A. Some of the opinions are the same. I have also added new opinions with respect to things that are specific to the UK and rebuttals of Dr Lee which obviously I did not have in Australia.

Q. You make no reference to the conversations with Mr Kosmynka, Mr Friedman or the other Apple employees in appendix B to your first report in these proceedings, do

you?

A. I do not.

Q. But you accepted in cross-examination in Australia that, with the benefit of hindsight, you would have identified those discussions in your report in the Australian proceedings?

A. To the extent that I would need to rely on those conversations, I would have included that.

Q. You would also accept that, with the benefit of hindsight, you should have identified those discussions in your reports in these proceedings?

A. I do not think so. I formed my opinions in these proceedings without referring or regard to those conversations.

Q. Okay, we will come back to that, Professor.

Let us go back to paragraph 10 of first Rubin, page 6, {C2/3/6}. You see that you say here that you had regard to Apple internal documents produced and provided to you, is that correct.? Do you see that?

A. Where exactly are you pointing?

Q. It comes about halfway down. You say, second sentence:

"These documents ..."

Etc.

Then the next line:

"... Apple internal documents produced in and

provided to me ..."

So that is in the list of materials?

A. Yes.

Q. Let us go back to appendix B. {C3/2/200}. Sorry for all the back and forth, Professor Rubin. If you flick through that, you will see that the only reference to any Apple internal documents comes under the heading we have just looked at. The first is Exhibit PS-2, Tab 12. Do you see that?

A. I am sorry, I missed a couple of words in there.

Q. I was saying that the only reference we see to any Apple internal documents is under the first heading, and it is the third bullet. It is Exhibit PS-2, Tab 12. Do you see that?

A. I see that.

Q. I think that is an erroneous reference. I think it should be PS-1, tab 12. It is an exhibit to Mr Schiller's statement. Is that correct?

A. I do not know, but it could be.

Q. That document is a presentation from December 2008. We can get it up on the EPE. It is {D1/48/1} and it is in tab 3 of your hard copy bundle, Professor Rubin. We have just got the cover email because it is a long document. You see it is an email from Ron Okamoto to Scott Forstall, and we see:

"Attached is a keynote preso outlining the various app commerce models ..."

Do you see that?

A. I see that.

Q. Attached to that email was a PowerPoint presentation about in app commerce, do you recall that?

A. In app commerce? That sounds familiar.

Q. But you do not refer to this document in the body of your first report, do you?

A. I do not know. I do not remember.

Q. Take it from me there is no reference in the first report.

Fifth bullet, page 200, exhibit CMF-1, and that is the exhibit to Mr Federighi's statement, yes?

A. I think so.

Q. So it is {B2/3/47}, tab 4 of your binder, Professor Rubin. It should be the penultimate page. If you flick right to the back, you can pick it up. Do you see the cover sheet to the exhibit?

A. Yes.

Q. Could I ask you to look through the list of documents quickly. (Pause)

A. I am sorry, I am not sure what the question was.

Q. I just asked you to look through the list of documents that you see in the index.

A. Okay.
Q. Just scan the index. (Pause)
A. Okay.
Q. These are all publicly available documents, are they not?
A. I think that they are.
Q. So they are not Apple internal documents?
A. Right.
Q. You have in fact not relied upon a single internal Apple document in preparing your first report; is that correct?
A. That sounds right.
Q. In your second report, Professor Rubin, you list 41 documents that you were provided with by Apple; is that correct?

We can pick it up in the appendix to the second report, it should be appendix B. Appendix B, pick it up at {C3/6/135}. They are not numbered but I counted them. There should be 41.

A. I am sorry, what is the question?
Q. The question is, you listed 41 documents that you were provided with in your second report, yes?
A. I also am not counting them but I will take your word for it.
Q. You will take my word for the next question, I hope,

which is that you referred to only five of those documents in the body of your report?

A. That is plausible.

Q. Back to first Rubin, paragraph 10. Let us pick it up at the sentence three lines from the bottom:

"Where I have relied upon witness statements ..." {C3/2/6}

A. I am sorry, you went too fast for me. I am not sure what you said.

Q. Sorry. First report, para 10.

A. Paragraph 10?

Q. Yes. Page 6.

A. Okay.

Q. So the same paragraph we looked at before but let us pick it up three lines from the bottom. You will see a sentence which begins:

"Where I have relied upon witness statements ..." Do you see that?

A. Yes.

Q. "Where I have relied upon witness statements, I identify below the ... parts of the witness evidence on which I have relied for each point. I exclusively depended on witness statements that I deem accurate, given their alignment with corroborating evidence from independent sources, and my academic and industry experience."

Yes?

A. Yes.

Q. You make extensive reference to Apple's witness evidence in your reports, yes?

A. That is correct.

Q. By my account, over 175 citations, does that sound about right?

A. I do not know, but I would not be surprised.

Q. You say here that you have only done so when you consider that evidence to be accurate, yes?

A. Yes.

Q. You say that you considered the evidence to be accurate if it aligns with corroborating evidence from independent sources or with your academic and industry experience, yes?

A. Yes.

Q. Many of the matters for which you rely on Apple's factual evidence relate to Apple's internal processes, yes?

A. That is true.

Q. For example, App Review?

A. That is true.

Q. Those matters are not public knowledge, are they?

A. I --

Q. I will restate: not entirely public knowledge?

A. That is correct.
Q. Presumably, you did not have knowledge or experience of them prior to your instruction by Apple as an expert witness?
A. I apologise, but I just have to hear that again.
Q. Presumably, you did not have knowledge or experience of the non-public matters prior to your instruction by Apple as an expert witness?
A. There may be things that I retained from previous cases, but I relied on things that I saw in evidence from this case, when I worked on this case.
Q. But for non-public matters, it would only be information that you had acquired in the course of these proceedings or other proceedings, yes?
A. These proceedings or other proceedings, yes.
Q. Professor Rubin, in a number of places in your report you note that your opinion aligns with opinions expressed by Apple's factual witnesses, yes?
A. Sure.
Q. I would like to look at a few examples. Let us go to first Rubin, para 173. That is {C3/2/90}. You say:

"From a review --"

Sorry, I am going too quickly, Professor Rubin. Are you there?

A. 173?

Q. 173, page 90.
A. Yes, I am there.
Q. You say:
"From a review of the Witness Statements of Apple executives in this case, it appears that Apple also concurs that centralised app distribution provides enhanced security benefits for the iOS platform."
Yes?
A. Yes.
Q. Let us go to 242, {C3/2/125}. If we go over the page -- sorry, no, back to page 125, pick it up at the start:
"I have discussed in section VII.C above how notarisation on macOS would not be sufficient to address the security needs of iOS Devices, especially given that iOS has a heightened security threat model. I note that Apple acknowledges that notarisation on macOS ensures a lower level of security than App Review. Mr Federighi acknowledges ... "
Yes?
A. Yes.
Q. Paragraph 250, page {C3/2/130}. Pick it up at the start:
"My review and analysis of Apple's security architecture, including the measures that it takes to conduct App Review on every app and app update

distributed through the App Store as discussed above, cause me to agree with Mr Federighi and Mr Schiller ..."

A. I see that.

Q. 290, page {C3/2/152}, you see:

"Consistent with my analysis, Mr Federighi observed during cross-examination in the Australia proceedings ..."

Then a quote from Mr Federighi.

Paragraph 331, page 169, {C3/2/169}. Near the bottom:

"It is my observation, consistent with Mr Federighi's statement in his witness statement, that IAP offers 'a secure payment mechanism for users and developers to transact --"

A. I am sorry, I did not see where you were.

Q. So it is page 169. We are in 331. Are you with me so far?

A. I am. It says:

"Separate and apart ..."

I am not sure where you were reading.

Q. Sorry, near the bottom, the final sentence on this page:

"It is my observation ..."

Have you got that?

A. Yes, I see that now.

Q. "It is my observation, consistent with Mr Federighi's

statement ..."

Then so on?

A. Yes.

Q. Then final example, 334, page 171 {C3/2/171}, and it is over the page on {C3/2/172}, pick it up about six lines from the bottom:

"Consistent with my opinion, I note that in the Australian proceedings brought against Apple by Epic Games, Mr Federighi testified ..."

Yes?

A. I should be better at this but I did not catch where you started.

Q. I have the advantage of a script, Professor Rubin, so it is not your fault at all. It is about six lines from the bottom.

A. Of page 171?

Q. We are on page 172.

A. Oh.

Q. It is paragraph 334, six lines from the bottom. You see the word "behaviour" and then a full stop, and then you will see:

"Consistent with my opinion ..."

A. Got it.

Q. Got it?

"I note that in the Australian proceedings brought

against Apple by Epic Games, Mr Federighi testified ..."

A. Yes.

Q. Nowhere in either of your reports or in the joint statement have you expressly disagreed with any of Apple's factual witnesses, have you?

A. I do not recall any disagreement.

Q. Professor, let us move on to the substance. If you go to paragraph 28 of your first report, that is {C3/2/12}.

A. Okay.

Q. We will see, if we pick it up about halfway down, third sentence:

"Security encompasses ..."

Do you have that?

A. I do.

Q. You say:

"Security encompasses issues like privacy, safety, trustworthiness, and reliability, as well as detecting and preventing malware, and entails protecting user privacy and the principles of consent, transparency, and minimisation, preventing unauthorised third-party access to protected data and privileged device functionality, protecting device reliability, and protecting against software piracy."

A. Yes.

Q. Your definition of security is broader than Dr Lee's

definition of security; is that correct?

A. Yes.

Q. That difference of opinion is most relevant to the question of whether objectionable content is a security risk, yes?

A. I think that it is relevant to that. I have not considered if it is the thing it is most relevant to.

Q. Whether objectionable content is a security risk is most relevant to whether different forms of app review, lower-case, so we are not talking exclusively about the Apple app review, are as effective as Apple's App Review, yes?

A. That is right.

Q. Turning to the threat model faced by iOS, Professor Rubin. You say that iOS has an extraordinary threat model, yes?

A. I do. I do not know if you are pointing to a specific sentence, but that is true.

Q. You can probably pick it up in 29, the second line. {C3/2/13}:

"As I discuss in further detail in section V.B below, iOS has an extraordinary threat model ..."

A. Yes.

Q. I think the reasons you have given, I am trying to summarise your evidence, is that there are 1 billion

active iOS Devices. Those devices are almost constantly on and connected to the internet. iOS device users frequently download apps, of which there are now more than 1.8 million available. IOS devices store and transmit financial, medical and private information. They have a device camera and a microphone. GPS hardware follows owners nearly everywhere they go, and those devices are portable. Is that a fair summary?

A. Yes, there is one more. I think it is in another section of my report but it is important. Which is that people have come to rely on their mobile devices in an emergency, like if they are driving a car late at night and they get a flat tyre. If their phone does not work because of some malware or problem with it, that could be a serious real world consequence.

Q. You say that the particular threat model faced by iOS Devices means that the app distribution restrictions and the payment system restrictions are required, yes?

A. Can I please hear that again?

Q. Of course. We will start with the definitions. So when I say the app distribution restrictions, do you know what I mean?

A. You are talking about Apple's requirement of distributing centrally?

Q. Yes.

A. Okay.
Q. Payment system restrictions?
A. Yes, IAP.
Q. IAP. The question is: you say the particular threat model faced by iOS Devices means that the app distribution restrictions and the payment systems restrictions are required?
A. Acquired?
Q. Are necessary.
A. Required. I am so sorry, it is the accent. I thought you said acquired. Yes, I think they are required.
Q. Required.
A. Yes.
Q. Let us pick up Mr Federighi's statement at paragraph 34. {B2/3/9}. It is the white bundle. Just to avoid any confusion, I am always going to give you the same page number that is stated at the bottom, so {B2/3/9}, you are looking for the 9 on the right-hand side.
A. Okay.
Q. We will pick it up just above 34. You will see in this section of the witness statement Mr Federighi is discussing iOS security and the threat model it faces, yes?
A. Yes.
Q. Just to get our bearings. Let us go to the bottom of

the page. 37, the final few words on the page:

"We envisioned iPhone as a device that would accompany its user everywhere ..."

Over the page {B2/3/10}, next sentence:

"iOS devices contain highly sensitive personal information - often more sensitive than that stored on a computer. For example, iOS Devices have sensor hardware - such as GPS hardware and Apple's Ultra-Wide (U1) chips for spatial awareness - that detects their users' location."

Have you got that?

A. Yes.

Q. A little bit further down, one sentence away:

"iOS devices holding this sensitive data, including financial and health data, are smaller than Mac devices and - with their microphones and cameras - are more likely than Mac devices to be with their users at all times."

A. I see that.

Q. Next sentence:

"... we wanted to radically re-think people's relationship with apps, so they would feel confident frequently downloading lots of apps to solve all kinds of problems ..."

Down to 39:

"From the threat model perspective, iPhones present a very attractive economic opportunity to attackers - more attractive than Mac devices. There are over a billion active iPhones - more than 10 times the number of Mac devices - in use globally, and their users are far more prone to download apps than typical for Mac or other personal computer (PC) users."

Then over the page, {B2/3/11}, 40, if I could ask you to read from:

"An iOS device is a very personal device ..."

Down to:

"... throughout the day."

So it is just a couple of sentences there. (Pause)

A. Okay.

Q. So you clearly relied on Mr Federighi's evidence in reaching your own conclusion that iOS Devices face an extraordinary threat model, yes?

A. Well, I am a user myself, so I had my own experience, and I have studied mobile security and taught about it and everything that Mr Federighi said is consistent with my opinion.

Q. But in your report at footnotes 78 and 79, that is pages 62 and 63, {C3/2/62-63}. So at the bottom of page 62, let us pick it up at paragraph 128 of the text. You see:

"The value of the data [etc]. It holds some of the user's most personal information [footnote 78]."

Then we see a citation to Mr Federighi at 40, yes?

A. Yes.

Q. Over the page, we will pick it up at the end of 128:

"The potential economic opportunity presented by an attack on iOS --"

A. I am sorry, you said page 128?

Q. Paragraph 128.

A. Paragraph 128.

Q. So it is the final part of the sentence on page 62:

"The potential economic opportunity presented ..."

Do you have that?

A. Yes.

Q. Then read over the page:

"... by an attack on iOS Devices exceeds that of an attack on Mac devices or PCs by orders of magnitude [footnote 79]."

Then it is "Id", which is a reference back to Mr Federighi's statement and it is paragraphs 39 to 41.

A. Correct.

Q. So you have expressly cited Mr Federighi's statement in support of the opinion you have given in your report, yes?

A. Correct.

Q. We saw that in paragraph 10 of your first report you have said that you have only relied on Apple's witness evidence where you were satisfied it was accurate, yes?
A. Yes.
Q. But in 2008 when Apple launched the App Store, there were not 1 billion iPhones, were there?
A. There were not.
Q. There were about 10 million?
A. I do not actually know, but I will take your word for it.
Q. That is from Apple's skeleton, paragraph 37(a). I do not think we need to turn it up, but for the transcript that is {A1/5/15}, so presumably correct, coming from the horse's mouth. In 2008 when the App Store was first launched, there were not 1.8 million iOS Apps, were there?
A. No.
Q. There were about 500. Again, Apple's skeleton, paragraph 27(e), {A1/5/11}.

So any threat model developed by Apple at around the time of the launch of the App Store could not have been based on the particular facts that there are now 1 billion iPhones and 1.8 million iOS Apps, could it?
A. I would say that the threat model obviously could not have assumed a billion phones and things like that, but

Apple saw the architecture of people with phones, and moving around a lot and having the phones with them, and understood basic principles like defence in depth, and applied those principles to the design, and then refined it over the years as the threat model evolved.

Q. The question, Professor Rubin, was whether or not Apple could have had regard to those particular facts?

A. No.

Q. But nonetheless, you thought Mr Federighi's evidence was accurate and you relied upon it, yes?

A. Yes.

Q. Professor Rubin, you would agree the evaluation of a particular device or systems threat model is a complex process?

A. For some systems, yes.

Q. For iOS, for example, it would be a complex process?

A. Yes.

Q. You would therefore expect the threat modeling exercise to be documented?

A. Yes.

Q. But you do not refer to any document which sets out Apple's evaluation of the threat model faced by iOS at the time of its creation, correct?

A. I did not refer to the threat model at the time of the creation of the iPhone.

Q. So the question was: you do not refer to any document which sets out Apple's evaluation of that threat model?
A. At the time of the creation?
Q. At the time of the creation.
A. That is right.
Q. You do not refer to any document which sets out Apple's evaluation of the threat model faced by iOS at the time the decision was taken to allow third parties to develop native apps for iOS, correct?
A. You are talking 2008?
Q. 2008.
A. Yes, I do not.
Q. In your deposition in the United States, you said it was clear to you, based on the conversations you had with Apple engineers, that Apple had large teams looking at the threat model facing the iPhone, yes?
A. Okay, it was four years ago, I do not remember what I said, but I agree with that.
Q. You have never asked Apple for any documents which reflected the work that it did evaluating the threat model faced by iOS?
A. I do; in my second report I have quite a few references to it. But I did not hear you say "at the time of its creation" in that version of the question, so I ...
Q. Sorry, you did not hear me say "at the time of its

creation"?

A. In that version of the question. So if you are just asking me at any time, I do have citations to those.

Q. I am afraid I am now confused, Professor Rubin.

A. Sorry.

Q. So your evidence is that you do refer to documents which document the threat modeling exercise, albeit those documents do not relate to the time of the creation of the iPhone or the decision to open up the App Store, is that ...

A. That is what I was trying to say, but you said it better than I did.

Q. But you agree that if there were any such documents, they would be useful to you in preparing your own report?

A. For the purpose of this case and these proceedings, I do not see the usefulness of threat modeling documents from 2008. I was looking at the threat models in the time of the Class period and today, and so I just -- that does not seem relevant to me.

Q. Professor Rubin, you refer to a document that you refer to for the first time in your second report. I think that document is going to be {D1/16}. This document is confidential, so I will be careful not to read anything out and you should do likewise. It is at tab 6 of your

bundle. The date of this document, I am told, is 15 August 2007, so around the time of the launch of the iPhone, yes?

A. That is correct.

Q. Do you recognise this document?

A. I am not sure.

Q. You refer to it at paragraph 172 of your second report, that is {C3/6/79}. Go over to 80 {C3/6/80} and pick it up about halfway down, after footnote 237. Again, it is confidential so let us not read it out, but you see:

"The [blank blank blank] for example, is a team of [blank blank blank]."

If you look at 238.

A. I see that now.

Q. You see the Bates number, you see it ends 735.

Back to tab 6, you will see it ends 735. So that is the document you refer to there, yes?

A. Yes.

Q. Do you know when you were first provided with a copy of this document?

A. (Pause). It was in the -- I am pretty sure it was in the summer, last summer.

Q. Before or after you were cross-examined in Australia?

A. After.

Q. Was it provided in response to a request you made of

Apple?

A. Yes.

Q. Turning to the substance of the document, are you familiar with the role performed by the team referred to here?

A. Yes.

Q. If we go to page 3 {D1/16/3} and pick it up near the bottom, you will see non-confidential words "Core OS"?

A. I see it.

Q. That is a reference to iOS, yes?

A. Yes.

Q. Could I just ask you to review the first bullet. I am not going to read it out but read it to yourself.

(Pause)

A. Okay.

Q. You would agree that that bullet point suggests that one of the tasks for this team was to create a document recording the threat model facing iOS, yes?

A. It does not specifically mention a document and -- I am allowed to reference words that are not in pink?

Q. Yes, you are.

A. So it says:

"Create a threat model ..."

A threat model can often be a document. What I see a lot of our consulting clients do is they use a threat

modeling tool, so it does not actually create a document, it just creates a file within that tool.

Q. Are you distinguishing between a physical hard-copy document and a file on a computer program?

A. I was distinguishing between a document and a tool in a particular state where you have done some modeling.

Q. Did you say a tool in a particular state? Can you explain what you mean by "in a particular state"?

A. Sure. So the easiest example I can give is like a computer network architecture diagram. Let us say I ask you to create a diagram of a network, and it would have a router, a server and a client machine. So you go into your account and you log in and you use this graphical editor to create that visual and then you save it and then you go away.

So I would not say you have created a document, but you can come back and load your work up and see that. So there are threat modeling tools which have that capability of letting you work through a software package to create a model, but it does not save it as a document.

Q. The key point, Professor Rubin, is that you can come back and load your work up and use the work you have done already as a reference point for future analysis, yes?

A. Yes.
Q. If we go over the page, the first bullet, it is not confidential, you say:
"Document current security mechanisms especially documenting their weaknesses and areas specifically not covered by design."
{D1/16/4}
This clearly calls for this particular team to create documentation, yes?
A. Yes.
Q. Let us go down to the heading again, not confidential, "Product Security". If I could ask you to look at the seventh bullet, which starts:
"Create a threat model ..."
A. Yes.
Q. Again, would you agree that that bullet point suggests that one of the tasks of this team was to create a document recording the threat model facing iOS?
A. It is the same answer. A threat model could be within a threat modeling tool or a document.
Q. But you would agree that one of the tasks for this team was to create a record?
A. That is fair.
Q. Or a reference tool?
A. That is fair.

Q. If this team within Apple was tasked with creating a record or reference tool or document, you would expect it to do so, yes?
A. I think so.
Q. Even after you received this document, you did not ask Apple if they had any further documents that this document suggests were created in and around 2007?
A. I made a substantial request of Apple for documentation they would have regarding threat modeling. This was one of quite a few documents that came back, but many of them are public documents, so I was given references to them.

You had me on page 77. If you look at some of the footnotes like on page 75, I list some of the threat modeling documents in the footnotes at the bottom. I think there are some on page 74 as well and 76 as well {C3/6/78-80}.

Q. The documents on 74/75 are directed at developers, correct?
A. I am sorry?
Q. The documents that are referred to on 74 and 75 are directed at developers, yes?

Let us pick it up at 169:

"Apple has also directed developers on considering threat models when designing software [footnote 232] ...

risk assessment and threat modeling ..."

A. Yes.

Q. So this is developer documentation?

A. This is documentation that is targeted at developers but it discusses the threat modeling that Apple has done.

Q. But it is not a document from 2007 and 2008 that shows Apple's internal threat modeling process, no?

A. Right.

Q. Let us look at one of the other documents which you were provided with at the time. If we pick it up at 173 of your second report, {C3/6/80}.

I am going to arrange myself, Professor. If you give me one moment.

A. Sure.

Q. You will see:

"In addition, according to my review of Apple documentation, I understand that Apple incorporated the threat modeling process when developing their systems and continues to consider the threat model when developing new functionalities and engaging in product design. For example, I have observed that threat modeling processes would be applied to design of ..."

Then there are various things which are confidential referred to there, yes?

A. Yes.

Q. I want to have a look at the document that you refer to in footnote 242. That is {D2/987/1} and it is tab 8 of your white bundle, Professor Rubin. We will pick it up on page 1. Again, this whole document is confidential so I will be careful. You should do likewise.

Do you recognise this document?

A. I think so.

Q. I am going to ask you some questions about it but they will be slightly opaque given the confidential nature, okay?

A. Okay.

Q. This is a formal documented threat model for a particular application created by Apple, yes?

A. Yes.

Q. That application forms only a small part of the overall iOS eco-system, yes?

A. That is true.

Q. But a formal documented threat model was created for it, yes?

A. (Pause). I am not seeing where it says that. I do not know.

Q. It is the nature of the document. Look at the -- if we look at the above the line next to the Apple symbol, which I assume is not confidential, you see the title of the document, and if we pick it up four paragraphs down,

you will see a description of what this document does.
A. Yes.
Q. Then fifth paragraph, if you read the sixth and seventh words it might help.
A. Which paragraph?
Q. Fifth paragraph. So you see a numbered list, 1-9.
A. Right.
Q. If you pick up in the paragraph below that. If you read the first few words to yourself, up to the comma.
A. Yes.
Q. So you would agree this is a formal documented threat model for that particular application?
A. Yes.
Q. Were you provided with a copy of this document at the same time as the August 2007 document we just looked at?
A. Most likely.
Q. After you received and reviewed this document, did you ask Apple if they had an equivalent document for the iPhone?
A. No.
Q. The App Store?
A. No.
Q. I want to consider the iOS threat model in comparison to Android and to Mac, okay?
A. Okay.

Q. Worldwide, there are more Android devices than iOS Devices, yes?
A. Yes.
Q. Android devices, like iOS Devices, are constantly on and connected to the internet, yes?
A. Yes.
Q. Android device users store and transmit financial, medical and private information, yes?
A. Yes.
Q. Android devices typically have a camera?
A. Yes.
Q. A microphone?
A. Yes.
Q. GPS hardware?
A. Yes.
Q. Android device users download lots of apps?
A. Yes.
Q. Two-factor authentication tokens are often sent to Android devices?
A. Yes.
Q. Android devices are often used in emergency situations like those you described for iOS Devices, yes?
A. Hopefully not often, but they are available for that.
Q. They are available for that. So in terms of device use and the information that the device handles, Android

devices and iOS Devices are in fact very similar?

A. True.

Q. Let us turn to Mac then. Mac devices store and transmit financial medical and private information, yes?

A. Yes.

Q. Confidential and proprietary information?

A. Yes.

Q. They typically have a camera?

A. The newer ones, yes.

Q. Microphone?

A. Yes.

Q. GPS hardware for the portable ones?

A. I do not think so. I have a one-year old Mac and there is no GPS hardware on its.

Q. To state the obvious, Mac laptops are portable?

A. Yes.

Q. Users often leave their Mac device in sleep mode rather than switching it off?

A. I do not know the answer to that but it makes sense.

Q. Two-factor authentications are also often sent to Mac devices?

A. Yes.

Q. I am going to suggest to you, Professor Rubin, that you have overstated in your reports the differences between iOS Devices and Mac devices when it comes to their use

case and the information they hold?

A. I disagree with that.

Q. Professor Rubin, in an earlier answer you referred to defence in depth, and I want to come on to discuss what you mean by defence in depth.

If we could pick up the joint experts' statement, which will be in the black binder and it should be behind the third tab. It is {C4/1/8} for the transcript. If we pick it up, I am afraid it is landscape which makes it more awkward still. Pick it up at the bottom, you will see "19 (Issue 1C.i)"., yes?

A. I see that.

Q. I am sorry, I will just take you to the heading further up the page. This is a summary of your main conclusions on the security expert issues, yes?

A. Yes.

Q. So we are in your section. What you say is:

"iOS implements a 'defence-in-depth' security architecture tailored to the particular threat landscape of iOS, where each layer of protection is designed to yield unique security benefits. IOS layers include Apple's App Review of every app and app update, centralised app distribution through the App Store and IAP for all digital goods and service transactions, in combination with other layers like on-device security

..."

App Review, centralised distribution and IAP are separate layers in Apple's defence in depth security architecture, yes?

A. Yes.

Q. You say that in addition to those layers, there are also on-device security protections, which are a combination of hardware and software protections, yes?

A. Yes.

Q. We can see a description of those if we pick it up at page 10 and it is paragraph 22. {C4/1/10}. Sorry, I misspoke, Professor Rubin, there is not a description there. We will pick it up in any event at paragraph 22. What we see is, this is the second paragraph:

"Security best practices call for layered defences - each layer strengthens the overall security posture of the system because an untrustworthy or malicious app must bypass all layers to reach an iOS device."

Do you see that?

A. Yes.

Q. Then paragraph 23, staying on the same page, picking it up about halfway through or a third of the way through the second line:

"... iOS App developers and iOS Device users enjoy the combined security benefits of all layers within

iOS's defence in depth security architecture. The combined security benefits have resulted in iOS being safer than other platforms, facing fewer attacks and malware infections than Android, Windows or macOS."

A. Yes.

Q. And you would agree, Professor Rubin, that the security of a given type of device is a product of the combination of security measures that it enjoys, yes?

A. I am not sure I understand the question.

Q. What we have just seen, Professor Rubin, is that Apple layers a number of different security mechanisms on top of each other. So if we start at the bottom, we have got hardware, we have got software, we have got App Review, and we have got centralised distribution, yes?

A. Right.

Q. What we saw in your summary of your conclusions is you say that iOS device users enjoy the combined security benefits of all layers?

A. Right.

Q. The question is when you are comparing two types of device, so take iOS versus Mac, the overall degree of security enjoyed by each type of device is a product of the combination of the different security measures that have been taken in respect of that device?

A. That and the threat model of each device.

Q. The threat model facing each device?
A. Yes.
Q. So that is true for a comparison of iOS and Mac, yes?
A. I would say so.
Q. It is true for a comparison of Android and iOS, yes?
A. Yes.
Q. Let us start with on-device protection. Let us go back to your first report, it is paragraph 159, it is {C3/2/82}, so internal page 82 for you, Professor Rubin. What I want to do is just quickly -- sorry, we will see the heading "Apple's On-Device Runtime Security Protections", so that is where we are in your first report, this is your description of those protections, and I just want to run through quickly each of the protections you identify, okay?
A. Okay.
Q. So the first is sandboxing, and sandboxing:

"... confines an application within a restricted environment to prevent it from accessing unauthorised resources or affecting other parts of the system."

Yes?
A. Yes.
Q. The second feature you identify, this is over the page, 160, digitally signed entitlements, yes? {C3/2/83}
A. That is a paragraph, yes.

Q. Yes, and you say the purpose of digitally signed entitlements is to provide:

"... further assurance that an app's permissions remain within the bounds of what has been officially approved, vetted, and could not be modified when the app is installed on an iOS Device."

Yes?

Q. Paragraph 161, mandatory code signing. We see:

"iOS requires that all executable code be signed using an Apple-issued code-signing certificate; otherwise, an app could not be run on an iOS device. Third-party apps must also be validated and signed using an Apple-[signed] certificate. Mandatory code signing extends the chain of trust from the operating system to apps - iOS users would be able to know that an app they install from the Apple App Store on iOS Devices is from a trusted source ..."

Then so on, yes?

A. Yes. Just you said "Apple-signed certificate", and it is an "Apple-issued certificate".

Q. This is in the second line, is it?

A. Third to the fourth.

Q. Ah, I misspoke. Thank you, Professor Rubin.

A. Sure.

Q. The code-signing that you are addressing here is the

code-signing that happens after App Review, is that correct?

A. Correct.

Q. Then 162, you see a discussion of the hardware security modules. The first that is identified is the Secure Element which:

"... stores payment information, such as account information associated with a payment card."

Yes?

A. Yes.

Q. Over the page {C3/2/84}:

"Apple iOS also utilises a Secure Enclave, which ... stores encryption and decryption keys and biometrics data utilised for Touch ID and Face ID authentication."

Yes?

A. Yes.

Q. You say further down:

"Under extreme circumstances, when the kernel is compromised, the Secure Enclave remains unaffected, preventing ... access to sensitive information ..."

Yes?

A. Yes, "unauthorised access".

Q. Is that true also of the secure element as opposed to the enclave?

A. I think the secure element has a tamper proof

functionality but I would have to look at the specs to refresh myself.

Q. In case it is helpful, Professor, the reason I ask is that you say just above that:

"... secure element and secure enclave are isolated from the main processor to provide an extra layer of security that keeps sensitive data secure even if an application processer kernel becomes compromised."

What was not clear to me is whether the sentence "under extreme circumstances", whether that was an extension of the point that you were making in that sentence. So it is really a clarification for my benefit.

A. I see. I would say yes.

Q. Again, for my benefit and the Tribunal's benefit could you give an example of the type of extreme circumstance you are referring to in the sentence that we have just looked at?

A. Sure. So what I talk about in the report is a kernel compromise. The kernel is the lowest level of the operating system that controls the functionality of the device so it is considered a complete and total compromise of a system if the kernel gets compromised.

What I am saying here is that Apple has added some hardware that protects critical information like

financial data even if the kernel is compromised. So a kernel compromise could occur if a piece of malware is able to exploit a vulnerability in the system and run hacker written code on the kernel, and so that is not something that is supposed to happen but that is why we have malware, malicious software, and when that does run and compromises the kernel the attacker still would not have access to credit card information for example because it would be in the separate secure hardware.

Q. Thank you, Professor Rubin. On to 163. You say:

"The Secure Enclave also includes a unique ID (UID) ..."

Then further down:

"Apple also uses Kernel Integrity Protection..."

Do you see that?

A. Yes.

Q. Then final item, 164:

"In addition Apple utilises Address Space Layout Randomisation (ASLR)... "

Yes?

A. Yes.

Q. If we go back to the joint statement, so that is the third tab in your black binder, and for the EPE it is {C4/1/33}, again, fighting with the layout for a moment. What we are interested in Professor Rubin is issue

1C.i-3. Do you have that?

A. Yes.

Q. The proposition is:

"Apple's hardware security and biometrics, and software security mechanisms will continue to provide security protections even if Apple's Restrictions are removed."

Two questions, Professor Rubin. The reference to "Apple's hardware security and biometrics, and software security mechanisms", does that refer back to the security protections we have just looked at in your first report?

A. Yes.

Q. Where it refers in that proposition to "Apple's Restrictions", that is a reference to what I call the app distribution restrictions and the payment system restrictions, yes?

A. Yes.

Q. Let us look at the responses to the proposition. The first column is Dr Lee, the second column is you.

Dr Lee says:

"I agree.

"They function independently of the app review process, app distribution model, and the ASPS."

Then across to you:

"I agree that these security mechanisms will continue to run in an alternative world where centralised app distribution, App Review, or IAP are not implemented on iOS."

Yes?

A. Yes.

Q. So a rare moment of agreement between you and Dr Lee that these security mechanisms, the hardware and the software mechanisms we have looked at, operate independently of app review, centralised distribution and the ASPS/IAP, yes?

A. Yes.

Q. If we just go to paragraph 225 of your first report. It is {C3/2/116}. Just pick it up at the start. I will give you a second, Professor Rubin. Sorry, I am going too quickly.

A. I have found it.

Q. 225 says:

"In Apple's Australian proceedings against Epic Games, Mr Schiller was asked whether 'most of Apple iOS security mechanisms are at a device level and would remain in place if Apple allowed direct downloading from developers as the Mac system does', to which Mr Schiller answered 'No'. Mr Schiller was then asked whether 'all of those device-level protections would remain in place

if Apple were to allow third-party iOS App stores', to which Mr Schiller also answered 'No'."

Then you say:

"Similar to my opinions, Mr Schiller's answers emphasise the reduced security and the expansion of attack surface if iOS Devices had to adopt the app distribution model and security measures of macOS."

Yes?

A. Yes.

Q. As we have seen, in fact, you do not agree with Mr Schiller, do you, because your opinion, as we have seen in the joint experts' statement, is that the hardware and software security measures on iOS Devices are independent of App Review, centralised distribution and the ASPS/IAP, yes?

A. So when we looked at, a minute ago, the joint report chart ... I do not know the right way to refer to you, if you are a learned friend or counsel.

The lawyer asking me questions, and I apologise if that is not an appropriate way to say it, only looked at the first paragraph of my response {C4/1/33}, and if we look below that I said:

"However, Apple's hardware security and biometrics, and software security mechanisms cannot fully replace the security benefits of centralised app distribution

model, App Review and IAP. Centralised app distribution model, App Review and IAP are still critical layers in iOS's 'defence-in-depth' architecture that yield unique security benefits."

So I think what I was saying here is that if you removed these layers, yes, the hardware would still be there and the software security layers would still be there, but they would not be as effective at providing security for iOS.

Q. If we just go back to 225. Let us pick it up at the second sentence at {C3/2/116}. Mr Schiller was then asked whether all of those device-level protections would remain in place if Apple were to allow third-party iOS App stores, to which Mr Schiller also answered no, and your answer to that question is yes, as we have seen?

A. I think the confusion is that I think they would be in place but they would not be as effective.

Q. You did not think it would be helpful to the Tribunal to point out that Mr Schiller was in fact incorrect about whether or not they would remain in place?

A. I think you would have to ask him what he meant by that.

MR KENNEDY: Sir, I am about to move on to another topic, so I do not know whether that is a convenient moment, before we launch into the vagaries of App Review.

THE CHAIRMAN: Yes. I will say ten minutes. Thank you.

(11.39 am)

(A short break)

(11.49 am)

MR KENNEDY: Professor Rubin, I now want to ask you some questions about Apple's App Review. I will start with an apology, because some of this is tedious even by my standards.

Let us pick it up in your first report, {C3/2/68}. I want to look in detail, I am afraid, at paragraph 140.

A. Okay.

Q. What I want to do, I am just going to go through it sentence by sentence, and I just want to understand the nature of the evidence and where it comes from, okay?

A. Okay.

Q. So let us start with the first sentence:

"Apple has a comprehensive manual and automated app review process for all apps and app updates submitted to the App Store - which, I understand from Apple's witness evidence, averages over 100,000 submissions per week globally."

That is simply a summary of Mr Schiller's evidence, is that correct?

Turn it up if it is helpful.

A. I am sorry?

Q. Is it simply a summary of Mr Schiller's evidence?
A. Yes.
Q. Then if we look at the second sentence:
"This App Review process plays a critical role in Apple's security mechanisms for making the App Store, 'a safe and trusted place for customers to discover apps, and a great opportunity for developers to deliver apps and services across iPhone, iPad, Mac, Apple TV, and Apple Watch in 175 regions' ..."
The first part of that second sentence simply quotes from some Apple marketing material, yes?
Again, we can turn it up if it is helpful.
A. The last part each time you said I could not catch.
Q. Sorry, I am saying that we can turn up the document in question if it is helpful.
A. Oh, I see.
Q. We can turn up Mr Schiller's statement, we can turn up the marketing material. If you think you do not agree with the question, you can say, well, let us look at the document. It is out of fairness to you, Professor Rubin.
A. I appreciate that.
So this is the -- it is from the developer App Store website, so I think you could call it marketing material or developer information.

Q. Footnote 103 which, for the transcript, is {D2/651/1}.
We see the text underneath the bold heading:
"The App Store is a safe and trusted place."
Those are the words that you quoted, yes?
A. Yes.
Q. Let us look at the second half of the second sentence, I think we should read in the words:
"App Review benefits ..."
Sorry, can we go back to {C3/2/68}. I am looking after footnote 103. I think the syntax should read in the words:
"App Review... benefits from over 15 years of improvements and innovations in response to the discovery and evolution of new safety threats."
Yes, do you see that?
A. Yes.
Q. Footnote 104, witness statement of Philip Schiller at 66. Let us turn that up. It is {B2/5/19}. In your white bundle, Professor Rubin, it is tab 18, and you are looking for page 19 at the bottom. It is probably the third page of the actual hard copy for you.
Have you got that?
A. Yes.
Q. Could I ask you quickly to read paragraph 66 of Mr Schiller's statement. I am afraid it is slightly

long. (Pause)

A. Okay.

Q. We see no mention here of improvements and innovations in respect of the discovery and evolution of new safety threats, do we?

A. (Pause). I do not see a discussion of the evolution of new safety threats in there.

Q. Let us look at the second citation, which is 78. It is page 22. It is a couple of pages forward for you, Professor Rubin. You will see a heading "Apple continually improves the App Store". Have you got that?

A. No.

Q. So we are in tab 18 of the hard copy. You are looking for {B2/5/22}.

A. Okay.

Q. It is paragraph 78.

A. I am there.

Q. It continues over the page, and can I ask you to read paragraph 78 to yourself. Again, I apologise for the length. (Pause)

A. Okay, I have read it.

Q. You will agree that only subparagraph (d) bears any relevance to what you say in paragraph 140 of your first report, yes?

A. I agree.

Q. That concerns a single development in 2016, yes?
A. Yes.
Q. It does not refer to 15 years of improvement and innovations in response to the discovery and evolution of a new safety threat?
A. I do think paragraph (d) at a high level is similar and consistent with what I say in paragraph 140.
Q. Okay. Let us look at the third sentence of paragraph 140, so back to {C3/2/68}, back in your first report, Professor Rubin. You say:

"As part of this process [this is App Review], Apple has developed sophisticated machine learning tools and a custom app review environment that automatically surfaces relevant and important facts and presents them to a human for review."

Footnote 105 cites to the statement of Mr Federighi. Let us open that up. It is {B2/3/23} for the EPE, and it is tab 4 of your white bundle, Professor Rubin, and you are looking for page 23 of the internal bundle numbering.

A. Okay.
Q. Could I ask you to read the paragraphs you cite, which are 80, 81 and 82 of that statement. (Pause).
A. Okay.
Q. No mention here of a custom app review environment that

automatically surfaces relevant and important facts and presents them to a human for review?

A. (Pause). These three paragraphs do not talk about the presentation to human review.

Q. Let us have a look at Mr Kosmynka's statement. It is {B2/6/21}, it is tab 56 of your white binder. Again, you are looking for internal page 21, Professor Rubin. We are interested in paragraph 80 when you get there.

A. Okay.

Q. Just so you have your bearings, we are in a discussion of the Columbus project. Are you familiar with the Columbus project?

A. Yes.

Q. Let us pick it up three lines from the bottom. This is not confidential so I can read it out:

"Another element [of the Columbus project] was 'assisted review', where computer tools would provide human beings with important information and facts, enabling them to make more accurate App Review decisions, and to do so more efficiently."

Do you see that?

A. Yes.

Q. If we could go to {H2/9/151}. This is confidential, Professor Rubin. This is the deposition of Mr Kosmynka in the Epic US proceedings, so 2021.

A. Is this in my binder?
Q. It is, sorry, my apologies. Tab 59. You will see a pink sheet which indicates confidentiality, and what we are interested in is page 193.
A. Okay, I have got it.
Q. What is being discussed here is the App Review process, and let us pick it up at line 22 on the left-hand side {H2/9/193}, and could you read lines 22-25.
A. Okay.
Q. I do not think that the word in isolation is confidential, but what we see is that Mr Kosmynka used the word "surface" in connection with that review, yes?
A. Yes.
Q. Let us go back to 140 of your first report, back to the third sentence which is where we started. {C3/2/68}

"... Apple has developed sophisticated machine learning tools ... automatically surfaces relevant and important facts and presents them to a human for review."

Do you see that?

A. Yes.
Q. Is this sentence based not only on Mr Federighi's evidence but also on your conversations with Mr Kosmynka?
A. I would not say it is based on the conversations.

I would say I probably forgot to cite his declaration in this case and perhaps his deposition testimony as well.

Q. You forgot to cite the deposition?

A. That is what I think, sitting here.

Q. Sorry, one point of clarification, Professor Rubin, when you say "his declaration in this case and perhaps his deposition testimony", what do you mean by "declaration"?

A. The previous tab that we looked at, was that not his statement in this case?

Q. That is his statement in this case, and that document is dated -- let us pick it up, it is 56 of the binder. It is dated 15 September 2024, and I think your first report is dated 15 May 2024?

A. Right. That would explain why I did not cite it. I think what I should have cited was the deposition testimony.

Q. Because you did not get it from Mr Federighi. You saw that, yes?

A. The paragraphs that I cite from Mr Federighi do not mention it, and Mr Kosmynka's deposition does, so I cited the wrong thing.

Q. Okay.

Fourth sentence:

"Apple's App Review 'is an essential line of

defence' that significantly contributes to iOS's security."

Do you see that?

A. Yes.

Q. There are two citations in the footnote. Let us go to the first one, it is {D1/1461/1}. It is tab 19 for you, Professor Rubin. It is not going to be that helpful to have it in hard copy but let us get it up anywhere.

Is it possible to search across the document for the word "essential"?

Take it from me, Professor Rubin, that the word "essential" and the word "defence" do not appear in that document.

A. Okay.

Q. Let us go to the second document you cite, it is {D1/1269}. Again, it is tab 61 for you, Professor Rubin, but not -- sorry, {D1/1289}, my mistake. This is the second document and, again, take it from me that the words "essential" and "defence" do not appear in that document.

A. Okay.

Q. So the quoted words do not appear in either document that you cite.

A. Correct.

Q. If we could go to {D1/1114}. This is 62 of your bundle.

The mystery is solved; we find the words on page ...

A. I am sorry, just give me a minute to get there.

Q. Of course. (Pause)

A. Okay.

Q. If you pick it up on page 2, you will see a bold heading "App Review"? {D1/1114/2}

A. Yes.

Q. Then you will see:

"The App Review team is an essential line of defence ..."

Do you see that?

A. Yes.

Q. That appears to be the document that you intended to cite, yes?

A. That looks right.

Q. If we go back to 140 of your first report{C3/2/69}, just look at the sentence again, fourth sentence:

"Apple's App Review is ..."

The question is: you are not expressing your own opinion here, are you?

A. In paragraph 140?

Q. In paragraph 140. You are simply quoting from Apple's document, yes?

A. I disagree with that. I am expressing my opinions here and I am using these documents and these statements from

witnesses as support.

Q. Can you see where the confusion arises as to whether or not that is your own opinion or simply a quotation from Apple's own document?

A. No.

Q. Let us look at the final part of 140. It starts:

"In 2022, for example, Apple's App Review rejected nearly 1.7 million apps or app updates. This includes rejecting more than 400,000 apps for privacy violations (such as asking for more user data than the app needs or mishandling the data the app collects), 29,000 apps for containing hidden or undocumented features, and more than 153,000 apps because they were found to be spam, copycats, or misleading to users in ways that manipulated them into making a purchase."

Do you see that?

A. Yes.

Q. You take these figures from Mr Schiller's witness statement, correct?

A. Yes.

Q. Did you ask Apple for any data or information underlying these figures?

A. No.

Q. So you have not formed your own view on their accuracy?

A. I am assuming that Mr Schiller represented that

accurately.

Q. We saw, Professor Rubin, that the final category you list are apps that were found to be spam, copycat or misleading to users, and I am going to emphasise these words, "in ways that manipulated them into making a purchase", do you see that?

A. Yes.

Q. Let us go back to Mr Schiller's statement. It is {B2/5/32}, and it is tab 18 for you, Professor Rubin, and it is internal page 32 that you are looking for. We are looking at paragraph 116.

A. Okay.

Q. You will see this is where you took the figure from, yes? If we look at (b):

"App Review rejected over 153,000 apps for being spam, copycats or misleading users."

Yes?

A. Yes.

Q. But Mr Schiller does not refer to apps being misleading to users in ways that manipulated them into making a purchase, does he?

A. He does not say that in that paragraph.

Q. Let us look at the underlying press release which is referred to in the body of Mr Schiller's statement at {D1/1461}.

Let us look at the first page. It is tab 19 of your hard copy; the next tab, Professor Rubin {D1/1461/2}:

"App Store stopped more than $2 billion in fraudulent transactions in 2022."

Let us go to page 4, and what we are interested in is the last paragraph. Do you have that? {D1/1461/4}

It starts:

"There are other reasons an app can be rejected for fraud."

A. Yes.

Q. You see:

"For example, over 153,000 app submissions rejected from the App Store last year were found to be spam, copycats, or misleading ..."

Yes?

A. Yes.

Q. Again, the underlying press release does not refer to apps being misleading to users in ways which manipulated them into making a purchase, does it?

A. It does not say that.

Q. So the inclusion of those words in 140 of your statement is an interpolation by you, yes?

A. (Pause). Yes, I do not see that I can say that the 153,000 apps were spam, copycats or misleading users, and the part I am saying I do not think I can say is "in

ways that manipulated them into making a purchase", because it is not in either of these documents. I would just take that out.

Q. Take that out?

A. Yes.

Q. Professor Rubin, there are 405 pages of reports in this proceeding from you alone. We have looked at one paragraph, and we obviously do not have time to go through each of them, but do you see the difficulty you placed me and the Tribunal in, in deciphering which parts of your reports represent your own opinion, which parts are simply factual background, and in that case, the latter case, what the basis for those facts are?

A. I see what you are saying. The parts where I have a footnote and I cite to a particular piece of evidence is intended to be me showing support for the rest of the text in there which is offering my opinion.

Q. Professor Rubin, you would accept that it is uncommon to express an opinion whilst also directly quoting from a document, going back to:

"Apple's App Review 'is an essential line of defence' ..."

A. I do not actually see the problem in providing an opinion and quoting other sources to support that opinion.

Q. Let us move on, Professor Rubin. Let us go to para 146 of your first report. That is {C3/2/73}. I am afraid this is a very similar exercise to the exercise we have just endured. Here we are addressing Apple's use of machine learning tools as part of App Review, okay?

A. Okay.

Q. Still in the section of your first report that explains Apple's App Review process, and I want to pick it up at the fourth sentence. It is about a third of the way down. It says:

"Apple's machine learning and heuristics ..."

Have you got that?

A. Yes.

Q. "Apple's machine learning and heuristics are based on Apple's insight into developers and past experiences to quickly extract large volumes of relevant information and subsequently present this information clearly and concisely to a human reviewer in order to facilitate the expedient and accurate review of apps."

Yes?

A. Yes.

Q. 132 is a citation to Mr Federighi's statement. If we could have that up, it is {B2/3/23}, tab 4 for you, Professor Rubin, and what you want is page 23 internal.

A. Okay.

Q. Let us pick it up at 80. What we see is, halfway through the second sentence:

"Apple has invested, and continues to invest, substantial resources in the development and improvement of its computer analysis for App Review, including by incorporating the use of machine learning and other ... technologies."

Yes?

A. Yes.

Q. Paragraph 81:

"The tools developed for App Review, which benefit from over a decade of data used to train machine learning algorithms to identify malicious apps or other potential issues, look at the app's configuration files and metadata ..."

Etc; do you see that?

A. I see that.

Q. There is no other reference to machine learning in that paragraph. I will just let you read the rest of the paragraph. (Pause)

A. Right.

Q. If I told you that there are no other references in the rest of paragraph 79-83 to machine learning, would you accept that?

A. I am willing to operate on that assumption.

Q. Mr Federighi does not say that Apple's machine learning tools quickly extract large volumes of relevant information, does he?
A. Can you point me again to where you are referring to?
Q. If you look at the second sentence, so you cite 79-83, yes?
A. Yes.
Q. I have asked you to assume that I am correct in saying that the only two references to machine learning are the second sentence of 80 and the first sentence of 81, yes?
A. Okay.
Q. Neither of those two sentences says, in terms, that Apple's machine learning tools quickly extract large volumes of relevant information, right?
A. That is what machine learning tools do, so ...
Q. Nor does Mr Federighi say that the information is presented clearly and concisely to a human reviewer in order to facilitate the expedient and accurate review of apps, correct?
A. He does not say it in those words.
Q. Let us go to Mr Kosmynka's statement again. It is {B2/6/14}. It is tab 56 for you, Professor Rubin. We are interested in paragraph 47 this time. The words we are interested in are more than halfway down, the sentence beginning "The ..." It is not confidential:

"The computer analysis phases gather information and then present it in an organised way for interpretation by human reviewers."

Yes?

A. Yes.

Q. We have seen that Mr Kosmynka's statement is dated 15 September 2024 and that your first report is dated 15 May 2024, yes?

A. Yes.

Q. Is this another instance when you have relied on your discussions with Mr Kosmynka in preparing your first report without making that clear?

A. No, I did not rely on the discussions that I had four years, four and a half years earlier with Mr Kosmynka.

Q. Let us go to the fifth sentence of paragraph 146. {C3/2/73}. You see:

"Apple can incorporate information regarding malicious or otherwise problematic apps into its machine learning tools and App Review process to improve detection of potentially problematic apps during future review."

Footnote 133 is a citation back to Mr Federighi's statement at 79-83 which we have just looked at, yes?

A. Yes.

Q. I have shown you the only two references to machine learning in those paragraphs?
A. Right.
Q. Mr Federighi does not say what you say in the fifth sentence of paragraph 146, correct?
A. I think Mr Federighi does imply that.
Q. Let us have a look at Mr Kosmynka's statement, paragraph 89, {B2/6/24}. This is confidential, Professor Rubin, so I am just going to ask you to read the first three sentences of that paragraph to yourself, paragraph 89. (Pause)
A. Okay.
Q. Same question: is this another instance where you have relied on your discussions with Mr Kosmynka without making that clear in your report?
A. No.
Q. The sixth sentence of 146, {C3/2/73}. I will give you time to get back there. We see:

"... when Apple's analytical tools determine that an app improperly collects location data --"

A. I am sorry, I am not with you.
Q. I am so sorry. Sixth sentence. We just looked at footnote 133. You will see a sentence that begins "For example"?
A. Okay.

Q. Yes? I just want to pick it up after the comma:

"... when Apple's analytical tools determine that an app improperly collects location data and sends such data to data brokers without user consent, this app is rejected."

Yes?

A. Yes.

Q. Let us go back to Mr Kosmynka's statement, {B2/6/20}. Tab 56 for you, Professor Rubin, internal page 20. You will see a paragraph non-confidentially starting "By way of example of this ...", do you see that?

A. Yes, 73.

Q. Yes, 73. Could I just ask you to read the paragraph to yourself very quickly. It is confidential, so do not refer to it in open court. (Pause)

A. Okay.

Q. Is this an example of a time when you have relied on your discussions with Mr Kosmynka without (inaudible) your report?

A. No.

Q. It is fairly specific information that is included in your report about a specific example of malicious behaviour, I have to be slightly circumspect in our description, and the only place we find that specific description of malicious behaviour is in Mr Kosmynka's

statement which was not available to you at the time you prepared your report. Did you guess? Got lucky?

A. No, I had information about these examples from things like Mr Kosmynka's deposition in the Australia case, as well as documents that I reviewed in the case that mention these things.

Q. You do not cite them in a footnote to paragraph 146, correct?

A. Correct.

Q. So we do not know where you got it from?

A. Correct.

Q. The seventh sentence of 146, {C3/2/73}:

"Data related to the violation and rejection is then collected to train Apple's machine learning tools, which would facilitate future recognition of location data subversion."

Yes?

A. Okay.

Q. Neither Mr Federighi nor Mr Kosmynka address the use of Apple's machine learning tools to recognise specifically location data subversion, do they?

A. I would have to look through there to answer that.

Q. Are you aware of any place in which they do say that? This is your report, Professor Rubin.

A. I would have to look. I am not aware.

Q. That sentence purports to be a statement of fact about something that Apple does:

"Data related the violation and rejection is then collected to train Apple's machine learning tools ..."

A. That is my understanding of how Apple's machine learning tools work. It is the same as how any machine learning tools work, is they collect data and they train on the data and then they can be used to identify it.

Q. The eighth sentence, paragraph 146 {C3/2/73}:

"Apple's App Review further benefits from its own specialised knowledge of its own hardware and software."

Do you see that?

A. Yes.

Q. Citation again to Mr Federighi's statement at 79. Are you here expressing your own opinion or are you simply summarising Mr Federighi's evidence?

A. Which tab was that in again?

Q. Mr Federighi?

A. Yes.

Q. Tab 4. It is {B2/3/23}, 79. The final sentence.

A. So what is your question?

Q. The question is: is the eighth sentence of paragraph 146 of your report a statement of opinion or simply a recitation of Mr Federighi's evidence?

A. Here I am reciting what Mr Federighi's statement was.

Q. Let us look at the ninth sentence. You say:

"These techniques and knowledge ..."

You are referring back to machine learning tools that you have been discussing and the knowledge of Apple's own hardware and software, correct?

"... cannot be easily replicated outside of Apple."

Yes?

A. Yes.

Q. I think that is a statement of your opinion, yes?

A. Yes.

Q. But you provide no reasons for that opinion here in paragraph 146, correct?

A. In that paragraph I do not provide any reasons.

Q. Nearly there. The final sentence:

"These tools also enable Apple to provide extremely fast and efficient App Review without facing the same extent of the accuracy tradeoff that third-parties would generally have to make."

Is that a statement of fact or a statement of opinion?

A. This is my opinion.

Q. Let us go to paragraph 151 of your first report, {C3/2/77}.

Sorry, let us go back to the last answer you gave. I asked:

"Is that a statement of fact or a statement of opinion?"

You answered:

"This is my opinion."

But again, you provide no reasons for that opinion in that paragraph, correct?

A. Well, the reasons for these last two sentences are supported by all of the text earlier in that section.

Q. There is no mention anywhere earlier in that section to the tools that are used by third parties?

A. I do not discuss that in that section.

Q. But in the final sentence, you are purporting to make a comparison between the extent to which Apple faces the accuracy trade off and the extent to which third parties face the accuracy trade off?

A. In the sentence that is all I say.

Q. But I have no idea what the basis is for that comparison. There is nothing that precedes it.

A. No, I was retained as an expert and I am providing an expert opinion here.

Q. But not expert reasons?

A. Not in that sentence.

Q. Let us go first Rubin, 151. {C3/2/77}. We are still in the section of your first report dealing with the app review process. Do you have that?

A. Yes.
Q. What we see is, first sentence:
"Apple's App Review process implements malware scanning."
A. I am sorry?
Q. 151.
A. Oh, 151.
Q. First sentence:
"Apple's App Review process implements malware scanning."
Yes?
A. Yes.
Q. Then you say:
"Malicious actors are constantly writing new malware ... Through its various tools, Apple can take information [etc]."
Then the conclusion:
"This method of malware scanning prevents many malicious apps from entering the App Store."
Yes?
A. I am sorry, you paraphrased a few words here and there as you were going really fast. Let me just read this paragraph.
Q. Take all the time you need, Professor.
A. Thank you. (Pause).

Okay, what is the question?

Q. The question is: you have not provided any empirical evidence of the number of malicious apps that have been prevented from entering the App Store by Apple's malware scanning, correct?

A. I do not have any numbers here.

Q. Or anywhere else in your reports?

A. I do not recall without searching.

Q. Let us go to your second report, paragraph 158. {C3/6/72}. It is in the second tab of the black binder for you, Professor Rubin.

A. Okay.

Q. Could I ask you to read that paragraph to yourself and then I am going to ask you some questions about it, okay? (Pause)

A. Okay.

Q. Let us pick it up in the second sentence, which begins "I anticipate ..."; do you see that?

A. Yes.

Q. You say:

"I anticipate that Apple's knowledge repository containing over a decade of knowledge from App Review is particularly relevant to App Review."

Yes?

A. Yes.

Q. Have you reviewed or examined any repository used by Apple for the purposes of App Review?
A. I did not.
Q. We see in that sentence a reference to "over a decade of knowledge from App Review", yes?
A. Yes.
Q. You make the same point in a number of places across your second report, that Apple is uniquely well-placed to review iOS Apps because it has over a decade of experience of doing so, yes?
A. I believe I say that in multiple places.
Q. Para 18, para 122, 123, 156, 157, 161, 162, 166 and 178.
A. I cannot verify that.
Q. -- control there for a decade.

Professor Rubin, you would accept that if the App Distribution Restrictions had never been in place, other app distributors, other iOS App distributors, might have the same amount of experience as Apple in carrying out App Review, yes?

A. Can I hear the first part of that?
Q. Of course. You would accept that if the app distribution restrictions had never been in place, other iOS App distributors might have the same amount of experience as Apple in carrying out App Review?
A. If there was another App Store that had the same volume

of apps and the same resources that Apple had to perform the analysis that they did, then theoretically I suppose there could be another entity that could have built a knowledge base like that.

Q. Even if the app distribution restrictions were only removed in 2015 -- so rather than 2008, 2015 -- those other iOS App distributors could have nearly a decade of experience, yes?

A. Again, I think, subject to the assumption that they have the same number of apps submitted, and the same resources and talent that Apple has, then they could have built up such a knowledge base.

Q. If they had that knowledge base, those other iOS App distributors would be able to leverage that experience, yes?

A. If that were possible and someone had a knowledge base like that, they could leverage it.

Q. Let us go to paragraph 159 of second Rubin, so it is just the next paragraph, and again, I just ask you to read that to yourself. {C3/6/73}. (Pause)

A. Okay.

Q. So you make a criticism of Dr Lee and the analysis that he has done, yes, and then you go on to say:

"I have therefore performed a more detailed analysis of these tools, based upon the evidence which Dr Lee has

himself referred to, and what Apple in fact does."

Yes?

A. Yes.

Q. Then in the paragraphs that follow, I will give you a second to look through them in a minute, you summarise evidence that Mr Kosmynka gave in the United States and evidence that he has given in these proceedings, and if I could ask you to look through paragraphs 160 up until 166. It may assist you to look at the footnotes whilst you do so. {C3/6/73-75}. (Pause).

A. How far did you want me to read?

Q. Just up until the end of 165 and we are going to have a look at 166 together, okay?

A. Okay, I have still got two pages to go.

Q. Take your time, Professor. We have got a day and a half to go. (Pause)

A. Okay.

Q. Let us go to 166 together, {C3/6/76}. You say:

"These proprietary tools developed by Apple for its App Review process each benefit from Apple's experience and expertise with the malicious apps and developers that have sought to infiltrate the App Store as well as Apple's internal knowledge of its own platform and functionalities, and therefore could not be developed or deployed with the same effect by a third-party."

Yes?

A. Yes.

Q. In reaching that conclusion, you have simply relied upon Mr Kosmynka's evidence, correct?

A. I mean, obviously my expertise and experience too, but in terms of the facts that I considered, I was relying on Mr Kosmynka's statement.

Q. You did not carry out a review of the code that comprises each of the tools you consider in these paragraphs?

A. Correct.

Q. You have not used the tools personally?

A. I did not.

Q. You have not seen them in operation?

A. Correct.

Q. You do not in fact, in the paragraphs you were just looking at, refer to any third-party tools, correct?

A. I do not discuss those specifically in this section.

Q. There is no basis for the conclusion in the final clause that those tools could not be developed or deployed with the same effect by a third-party, correct?

A. There is a basis for that.

Q. What we have seen, Professor Rubin, is that you simply summarise Mr Kosmynka's evidence, which considers only Apple's tools, yes, and we see simply the conclusion

that third parties could not do it?

A. Right, but I am familiar with the tools that -- with many of the third-party tools, so I am able to make that conclusion.

Q. Again, Professor, you see the difficulty that I am in and the difficulty that the Tribunal is in. You may well be familiar with the various tools, but you do not refer to them here. You do not say -- let us take an example -- DT App Analyser does X. Product Y produced by company Z is similar but deficient in respect to A, B and C, do you?

A. Right, so one of the issues with integrating third-party tools is that Apple built a pipeline of their process, so they take concepts that exist in some third-party tools but they have been specialised to feed into each other and so my point is you cannot just take third-party tools and plug them in and expect them to work in a pipeline that is been very customised and developed with that intention.

Q. But the import of the conclusion you present, Professor Rubin, is that a third-party could not develop or deploy its own tools to the same effect as Apple and no basis for that conclusion is presented in the paragraphs that precede it?

A. I do not agree with that assessment.

Q. Let us move on to human review as part of Apple's App Review. What I would like to do is I would like to summarise what I understand your evidence to be about human review, okay?
A. Okay.
Q. I am going to ask you some questions. I will take it one by one and you can say yes/no, accurate/inaccurate for each one, okay.
As I understand it, your evidence is that human review is more adept at protecting against social engineering attacks, yes?
A. That is correct.
Q. When I say more adept I mean as compared to computer software tools?
A. That is what I assumed.
Q. It is better positioned to determine whether an app will do everything it promises to do, yes?
A. I agree with that.
Q. Better positioned to determine whether an app contains hidden or undisclosed behaviour, yes? If at any point you would like to see the reference I have the references to your report. I can take you to them.
A. That is fine.
Q. You just have to agree.
A. That is fine. I just wanted to consider it and give it

some thought.

Q. Of course.

A. Yes, I agree with that.

Q. Better positioned to determine new types of threats and issues?

A. I agree with that.

Q. Finally, better positioned to determine whether user generated content is offensive or whether it violates restrictions on content in apps for children constitutes false or misleading content or seeks information in violation of privacy guidelines?

A. I agree.

Q. So let us take them in turn. Let us start with social engineering and whether an app does everything that it promises to do. What I would like to do is I would like to look at Dr Lee's second report which is {C2/13/21} and Professor Rubin, it is tab 50 of the white bundle for you and you are looking for page 21 in the bottom right-hand side. We are going to pick it up at paragraph 35. Just have a look at 35 -- sorry, if we go to page {C2/13/19} just so that we get our bearings.

A. Okay.

Q. What you say is:

"My response to the specific claims Professor Rubin makes regarding the necessity of App Review (in

particular, human review), including comparison with Apple's on-device and runtime security mechanisms is as follows ..."

What we will see is that Dr Lee goes through each of these items and he sets out his opinion.

I want to pick it up, page {C2/13/21} and it is the bullet which starts:

"Human review is no more effective than automated review/on-device security mechanisms at identifying social engineering attacks."

I want to pick it up in the third sentence which begins "while". It is about five lines down. Have you got that?

A. Yes.

Q. What Dr Lee says:

"While human reviewers can help identify obvious social engineering attacks, evidence shows that human review has often not been successful in identifying sophisticated engineering attacks on iOS Devices. It is not surprising that human reviewers have failed to identify non-obvious social engineering attack apps, for example, those which use a recognisable brand name to encourage users to install malicious apps, such as the recent example of the ChatGBT app."

Let us have a quick look at the ChatGBT. It is

{D1/1462/1} and it is tab 63 for you. If we just pick it up in the -- have you got that? You see it is a headline, "Scammers exploit AI trend". It is the web page.

A. Yes, I see that.

Q. Let us just pick it up in the first paragraph starting "Sophos researchers". Then let us look at the third sentence:

"Because the free versions have near zero functionality and constant ads, they coerce unsuspecting users into signing up for a subscription that can cost hundreds of dollars a year."

Yes?

A. I see that.

Q. That is an example of fleeceware; is that correct?

A. Yes.

Q. Fleeceware is a form of social engineering attack, yes?

A. Yes.

Q. Although Dr Lee describes this attack as non-obvious, it would be fair to say that it is not a sophisticated attack?

A. It could be sophisticated in certain ways, but it is pretty clear to a security expert if it is named ChatGBT instead of ChatGPT that something is wrong there.

Q. It would be clear to a human reviewer within Apple that

a reference to ChatGBT was trading on the name of ChatGPT?

A. That would raise a flag I think.

Q. From the description we see in this article these apps were clearly rubbish, they were junk?

A. Yes.

Q. Near zero functionality, and constant ads, and it is your evidence that human review is better positioned to protect against social engineering attacks, yes?

A. Yes, it is not perfect, but it is better than what a computer can do.

Q. Better positioned to determine whether an app will do everything it promises to do, yes?

A. Yes.

Q. This is an example of a time when human review failed to prevent this attack, yes?

A. Right.

Q. Cryptojacking is another form of social engineering, correct?

A. Yes.

Q. If we go to second Lee, paragraph 35, {C2/13/23}. I am afraid the use of bullets makes it slightly difficult to navigate, but ... we want to pick it up in bottom of or halfway through page 22, {C2/13/22}. You will see:

"Human review may be more effective than automated

review on-device security mechanisms at evaluating motivations ..."

Yes?

A. Yes.

Q. If we go to the top of page {C2/13/23}, we see:

"There have been multiple cases where human review has failed to detect harmful apps including the malicious Ace Pro and MBMBitScam iOS Devices apps that used crypto currency trading as a cover to steal money deposited by users."

Yes?

A. I see that.

Q. The attack described there using crypto currency trading as a cover to steal money deposited by users is another example of a social engineering attack, yes?

A. Yes.

Q. Another attack that was missed by Apple's human App Review, yes?

A. It seems that way.

Q. It has a hidden behaviour which is at the bottom of the page, this is the sixth bullet point, page 23. You see the heading:

"Human review is no more effective than automated review/on-device security mechanisms at determining whether an app contains hidden and/or undisclosed

behaviours."

A. I see that.

Q. The second sentence:

"If an app is submitted to App Review containing hidden or obfuscated behaviours, human reviewers may not test the app in the way that will trigger those behaviours; that is, they may have no better chance than automatic tools."

If we go over the page pick it up at the second sentence:

"For example, Apple had to issue a security update for iOS and macOS to patch an image processing vulnerability identified by the University of Toronto."

Known as the BLASTPASS bug, yes?

A. Right.

Q. Dr Lee is right, is he not, that whether or not human review identifies hidden behaviour is essentially a question of chance?

A. Well, there is always a probability of identifying or missing a piece of malware or a social engineering attack. The point that I was making is that in general humans are better at spotting these types of things such as hidden functionality or hidden behaviour than a computer would be because computers run algorithms, so you are going to have to know in advance what you are

looking for; whereas a human can look at something and see that something might be wrong, and so really the strength is in the combination of the human and the computers doing the review.

Q. You would agree that whether or not humans are better at identifying any particular form of hidden behaviour or attack will depend on the nature of the specific attack, yes?

A. Yes.

Q. If we just quickly go back to Dr Lee's fourth bullet, which is page 22 above the heading concerned with motivation. {C2/13/22}. About two-thirds of the way down you will see a sentence beginning, "For example the Jekyll app..." Do you see that? Some of the words are confidential so I am not going to read them out.

A. Wait, sorry, I was looking too low. So you want me to start where it says, "For example the Jekyll app"?

Q. Exactly. Just remember that anything pink is confidential.

A. Right. (Pause). Okay.

Q. That is an example of an app that had hidden behaviour, yes?

A. Yes.

Q. An example of an attack that neither a computer review or human review detected, right?

A. Right, this one slipped through the cracks.
Q. Overall, Professor Rubin, you do not present any empirical evidence as to the relative efficacy of human review versus computer review in identifying hidden app behaviour, do you?
A. No, I do not think that is something that could be measured like how much more effective is human review or computer review. But I do believe that running human review in concert with computer review that has been specifically designed to facilitate human review is the best way to review apps.
Q. Professor Rubin, there is a specific guideline under the App Review Guidelines that prohibits hidden functionality, yes?
A. That is right.
Q. Are you aware that when Apple rejects an app it tags the app with the reason for the rejection in accordance with the guidelines, yes?
A. Yes.
Q. So when an app was rejected for failing to comply with the hidden functionality guideline that would be recorded, yes?
A. Yes.
Q. Do you know whether that would be recorded -- I will restate the question. Do you know whether the record

would indicate whether or not the hidden behaviour was identified by computer review or by human review?

A. I do not know.

Q. New types of threat. I put my bundle away prematurely. It is second Lee, para 35, second bullet. Still in tab 50 for you. It is {C2/13/20} for the EPE.

A. I am sorry, that went too fast.

Q. We are staying in second Lee. It is paragraph 35. It is tab 50 for you and we want the second bullet point. So we are going to be on page 20.

A. Got it.

Q. We see:

"Human review" [this is in bold] is no more effective than automated review/on-device security mechanisms at detecting new types of ... threats."

Do you see that?

A. "New types of issues and threats", yes.

Q. "Issues and threats".

I want to pick it up. Right at the bottom you will see that on the last line you will see the word "Human".

A. Yes.

Q. You see Dr Lee expresses the view that:

"Human review is limited as human reviewers rely on their own knowledge, experience, consistency, interpretation and recall, which often does not extend

to new or obfuscated attacks."

Yes?

A. I think that could be a limitation of human review.

Q. The final category that we started of my summary of your evidence, the final category was offensive user generated content, content in apps for children, so inappropriate content in apps for children. False or misleading content or information sought in violation of privacy guidelines, yes?

A. That sounds right.

Q. Each of these examples is only a security issue in the broader sense in which you use it as opposed to Dr Lee, yes?

A. Can I please hear the list again now that I have your question?

Q. Of course. Why do we not do it one by one and you can tell me whether you agree with the proposition?

A. Okay.

Q. Offensive user generated content?

A. Okay.

Q. Content, inappropriate content in apps for children?

A. Okay.

Q. False or misleading content?

A. So I think false or misleading content would include social engineering attacks which are one of the main

security issues.

Q. We have had a look at social engineering already, yes?

A. Yes.

Q. The final one was information sought in violation of privacy guidance?

A. Yes.

Q. So we are not concerned here with malware in the narrow sense, correct?

A. I do not think you listed anything there that relates to malware.

Q. Let us go to the second Rubin, paragraph 123.

Sir, I am conscious of the time. Perhaps if we just finish this question and that would be this topic finishing. One moment, sir, just to ...

THE CHAIRMAN: How long will that take you?

MR KENNEDY: Four or five minutes, sir.

THE CHAIRMAN: Yes, go ahead, thank you.

MR KENNEDY: Sorry, Professor Rubin, we were at second Rubin, paragraph 123 which is {C3/6/54}.

A. Okay.

Q. If I just ask you to read that to yourself quickly.

(Pause).

A. Down to 124.

Q. Yes. (Pause).

A. Okay.

Q. In this paragraph you are responding to Dr Lee's evidence on the efficacy of the human review element of Apple's App Review, yes?
A. Yes.
Q. Your evidence here is summarising Mr Kosmynka's evidence, yes?
A. I rely on some statements by Mr Kosmynka to form my opinions.
Q. So you are saying this does represent your opinion?
A. I do not understand your question. My report is here to represent my opinions in this case and so ...
Q. The question is whether you are simply summarising Mr Kosmynka's evidence or also expressing your own opinion.
A. I am expressing my opinions here and using Mr Kosmynka as support.
Q. You suggest, Professor Rubin, that Dr Lee does not take into account the tools and processes used by Apple as part of App Review. You say: "Dr Lee does not address these factors." This is the penultimate sentence.
A. Right.
Q. But you are aware that in his first report, Dr Lee does address his understanding of the tools and processes used by Apple as part of App Review, yes?
A. I recall him discussing them in his first report.

Q. He put in a third report that responded to Mr Kosmynka's evidence on those tools and processes, yes?
A. Right.
Q. Then the final sentence:
"Dr Lee provides no evidence to support his claim that Apple's App Reviewers achieve a specific level of efficiency at the expense of accuracy."
Do you see that?
A. Yes.
Q. We saw earlier in paragraph 146 of your first report a reference to the accuracy trade off, do you recall that? You can turn it up. It is page {C3/2/73}.
Final sentence:
"These tools also enable ..."
A. Right.
Q. So would you agree with the statement of general principle that there is a trade-off between accuracy and efficiency when it comes to software analysis?
A. Yes.
Q. You do not present any empirical evidence on the relationship between accuracy and efficiency in the context of Apple's human review element of App Review?
A. Right, I do not see how one would measure that but there might be ways that it could be done.
Q. Are you aware that App Review has something it calls the

SLA, the Service Level Agreement?

A. Yes.

Q. That is that they commit to, I am going to mis-remember the stats, but they commit to reviewing 80% of all apps within 24 hours and 90% within 48 hours or something, yes?

A. That is either correct or close.

Q. You are aware that Apple monitors the accuracy of the decisions that human reviewers make?

A. I am not sure I was, but --

Q. Take it from me --

A. -- I would not be surprised.

Q. -- and we can have a look at them later if needs be, but they monitor that.

A. I accept that.

Q. They monitor the time it takes human reviewers to make these decisions.

A. I accept that.

Q. So would you accept that data would or might be available that would allow you to assess empirically the trade-off between accuracy and efficiency in the context of Apple's human review element of that review?

A. I am not sure that is what the data would tell me but --

Q. But you have not looked into it?

A. No.

MR KENNEDY: Sir, that would be a convenient moment.
THE CHAIRMAN: Thank you. In terms of timing, how are you doing?
MR KENNEDY: We are on page 41, sir, of 84, so we are almost bang on halfway.
THE CHAIRMAN: Good. In that case we do not need to start before 2 then.
MR KENNEDY: No, sir.
THE CHAIRMAN: Dr Rubin, while we are breaking, so we are going to break until 2 o'clock, you are not to discuss your evidence with anybody else, please.
A. Okay.
THE CHAIRMAN: Thank you.
(1.05 pm)
(Luncheon Adjournment)
(2.00 pm)
THE CHAIRMAN: Yes, Mr Kennedy.
MR KENNEDY: Good afternoon, Professor Rubin.
A. Afternoon.
Q. You are still on App Review for a couple more questions and then I am going to move on.
Professor Rubin, in your first report at paragraph 240, you say that not all third-party marketplaces necessarily share the same goals or resources as Apple, nor do they all have goals or

priorities necessarily aligned with those of Apple, yes?
We can turn it up. It is {C3/2/124}.
A. Right.
Q. But would you accept that it is possible for a third-party marketplace to carry out a more comprehensive and more effective app review than Apple?
A. So your question is if it would be possible for a third-party app store to carry out a more comprehensive review than what Apple does?
Q. Yes.
A. I do not know that such a third-party app store would have the resources, but theoretically I suppose something like that would be possible.
Q. You are familiar with the Steam platform, yes?
A. Yes, the gaming platform.
Q. Steam conducts both computer review and human review of the games that are submitted to the platform, yes?
A. I think so.
Q. Steam has stated that its manual review of the game build is typically between three and five business days. Are you familiar with that?
A. I am.
Q. Malware is extremely rare on Steam, correct?
A. I am not certain.
Q. Let us have a look. Can we go to {G1/11/1}. This is an

expert report prepared in the context of the Epic Australia proceedings, and it is a report of Professor Anil Somayaji who was instructed by Epic in those proceedings. Do you recall that?

A. Yes.

Q. If we go to page {G1/11/64}, we should see a table 5, "Distribution Platform Curation Comparison", and this table compares the different app review and developer vetting processes across different platforms, do you see that? We have iOS App Store, macOS on the left-hand side, yes?

A. Yes.

Q. If we go over the page, {G1/11/65}, we should see Steam and then -- so Steam for Windows on the left-hand side. If we go to the farthest right column, we will see:

"I am aware of only one incident of malware being distributed on Steam ... in 2018 ..."

You are aware of this information due to your involvement in the Australian proceedings, yes?

A. Right.

Q. But you make no mention of Steam or Steam's app review process in your own reports, correct?

A. Correct.

Q. Moving on, Professor Rubin, to the relationship between centralised distribution and Apple's App Review. Were

you in court last Wednesday when I cross-examined Mr Federighi?

A. Yes.

Q. You will know, then, that Mr Federighi's evidence was that in the absence of the app distribution restrictions, Apple could and would review all iOS Apps for distribution in the United Kingdom against the full set of App Review guidelines, yes?

A. Yes.

Q. So it follows that centralised distribution through the App Store is not necessary to ensure that every iOS App goes through the initial Apple App Review process, yes?

A. Correct.

Q. What I want to do, therefore, is I want to ask you some questions about what you say are the benefits of centralised distribution as distinct from App Review, okay?

A. Okay.

Q. For the purposes of the questions that follow, I want you to assume that Apple is carrying out App Review of all iOS Apps regardless of where they are ultimately distributed against the full set of App Review guidelines. Okay?

A. Okay.

Q. That is the premise. Before I do that, I just want to

cover off one ancillary point. In your first and second reports, you say that a number of security consequences flow from the fact that under notarisation for iOS, under the DMA regime, Apple is only enforcing a subset of the full App Review guidelines, yes?

A. Yes.

Q. You would accept that those security consequences would not arise if Apple was instead applying the full App Review guidelines?

A. Yes.

Q. Let us pick it up, your first report, at page 78, that is {C3/2/78}. It is your black binder. You are going to see a heading, I hope, right at the bottom of the page, "(b) Other Benefits of Centralised App Distribution". Heading (a) on page 68 is "Apple's App Review", so we are now moving to what you describe as the non-App Review benefits of centralised distribution, yes?

A. So am I on page 78 or 68?

Q. We are on 78 for the other benefits. We are on 68 just so you can see the previous heading, just to help you get your bearings.

A. Okay, got it.

Q. Okay. So we are on 78, and let us start with para 155 over the page on 79. {C3/2/79}. We see:

"With centralised distribution, Apple effectively takes steps to prevent repeated instances of malware from entering the iOS platform. For example, App Review can, after identifying one app that contains malicious functionality, determine whether other apps submitted to the App Store also contain that malicious functionality, share a binary, or utilise the same tools that likely embedded the malicious functionality."

Yes?

A. Yes.

Q. In a world of decentralised app distribution and mandatory app review, after identifying one app that contains malicious functionality, Apple could determine whether other apps submitted for app review in the past also contain malicious functionality, share a binary, or utilise the same tools that likely embedded the malicious functionality in the original app, correct?

A. Under the assumption of a full app review, yes.

Q. Apple could review any future apps submitted to App Review for the same malicious functionality?

A. So in this assumption we are assuming that App Review is centralised?

Q. Yes.

A. Yes, so then my answer is yes.

Q. -- malicious functionality. My first question was: you

could review the back catalogue and you could identify whether the other apps had the same malicious functionality. My second question was: as new apps are coming into the centralised app review function, you could review those apps for the same malicious functionality, yes?

A. Yes.

Q. Apple could reject any apps that were found to contain that malicious functionality, yes?

A. Yes.

Q. The second benefit you identify is at 156 and 167. Let us pick it up at 156:

"Centralised app distribution allows Apple to obtain information in advance about iOS App developers. The information that Apple requires developers to submit when enrolling in the Apple Developer Program, Apple Developer Enterprise Program, or iOS Developer University Program, can assist in security protection efforts."

Yes?

A. Yes.

Q. Let us go to the joint statement. It is {C4/1/94}. It is in the third tab of your hard copy binder, Professor Rubin. What we want is issue 3B-10.

Professor Rubin, I am missing a page and so I am

just going to have to use the screen.

You see the proposition is:

"Apple could continue to enforce mandatory developer verification and mandatory code signing using certificates issued by trusted authorities, as well as implementing other measures [and so on]."

Yes?

A. Yes.

Q. If we see the next column is Dr Lee:

"I agree.

"These policies ... are orthogonal to the app review process and app distribution model."

Then the next is you:

"I agree that Apple could continue to enforce these security mechanisms in an alternative world where apps can be distributed through websites and third-party app marketplaces."

Yes?

A. Yes.

Q. So in the counterfactual world that we are discussing, it would be possible for Apple to require all developers of iOS Apps to register with Apple before permitting them to distribute iOS Apps even if Apple permitted distribution of iOS Apps otherwise than through the App Store, yes?

A. Yes, that works in this counterfactual.
Q. In fact, that is what Apple has done under the DMA regime, yes?
A. That is my understanding.
Q. If all apps are required to be submitted to App Review, Apple could continue to reject apps from a developer that has proven to be malicious, yes?
A. Yes.
Q. Apple could use developer information for other attribution purposes, yes?
A. Yes.
Q. Or when certificates are being abused?
A. Yes.
Q. Apple could remove from the App Store any apps associated with a malicious developer, yes?
A. From their App Store?
Q. From the Apple App Store.
A. From the Apple App Store, yes.
Q. Apple could ask other app stores to remove those apps from their app stores, yes?
A. I assume if Apple knew who all the app stores were that were hosting, they could ask that.
Q. In any eventual, Apple could revoke the signing certificates of malicious developers, yes?
A. Yes.

Q. That would prevent the malicious app from being run on an iOS device regardless of distribution source, yes?
A. Yes.
Q. If there continued to be mandatory developer registration for all iOS App developers, Apple could ultimately terminate a malicious developer account, yes?
A. Yes.
Q. If we look at the fifth sentence in first Rubin, para 157 at {C3/2/80}, what we want is the fifth sentence which begins right at the bottom of the page at 80:

"However, bad actors ..."

Have you got that?
A. Not yet.
Q. The final word on page 80, "However".
A. Got it.
Q. "However, bad actors have sought to avoid or circumvent Apple's rejection or account termination by acquiring multiple Apple Developer ... accounts."

Do you see that?
A. Yes.
Q. We see footnote 171. You say:

"Based on my understanding of the malicious actors and identity vetting in general, attempting to acquire multiple accounts is a common practice of malicious actors. My understanding aligns with the witness

statement of Mr Philip Schiller at [116]."

If we just turn up paragraph 116 of Mr Schiller's statement, it is {B2/5/32}. It is tab 18 in your hard copy bundle, Professor Rubin. We are looking for page 32 internal.

A. Okay, I'm there.

Q. We are at 116, and we want subparagraph -- forgive me, Dr Rubin, one second. Subparagraph (h):

"428,000 fraudulent developer accounts were terminated."

Yes?

A. Yes.

Q. He just refers here to fraudulent accounts, he does not refer to multiple accounts, correct?

A. Right.

Q. The second reference you give is to Mr Federighi's witness statement at 120, which is {B2/3/37}. It is tab 4 for you, Professor Rubin. Internal page 37.

A. Okay.

Q. I think it is a bad reference, because this is about qualifying for the Apple Developer Enterprise Program. Do you see that?

A. Yes.

Q. The correct reference I think is meant to be 123 which is over the page on {B2/3/39}. Can I just ask you to

read paragraph 123 to yourself. (Pause)

A. Okay.

Q. Again, Mr Federighi says nothing about developers attempting to create multiple accounts here, correct?

A. He says fake developer identities, not multiple.

Q. So when you say "bad actors have sought", you are not referring to any actual instance on iOS, correct?

A. I am assuming that some of the fake developer identities would be bad actors creating multiple accounts.

Q. Let us go to your second report, paragraph 130. {C3/6/58}

A. Okay.

Q. You say:

"Furthermore, where Apple continues to perform its full App Review upon apps available in the App Store, but other app marketplaces conduct lower levels of review, 'it could become more fruitful for malicious developers to seek to impersonate a legitimate developer or otherwise seek to mislead users into believing that Apple has conducted its full App Review on an app'."

Yes?

A. Yes.

Q. You are quoting from your own first report, yes?

A. Yes.

Q. If an app is submitted to Apple for App Review before

distribution through a third-party marketplace, so a centralised App Review, any attempt to impersonate a legitimate developer should be identified by Apple at that stage, yes?

A. It would be the same process or the same result.

Q. The premise of your 130 in your second report was fully decentralised distribution with decentralised App Review, yes?

A. Decentralised App Review?

Q. I believe so. You see:

"... where Apple continues to perform its full App Review upon apps available in the App Store, but other ... marketplaces conduct lower levels of review ..."

A. Okay, yes.

Q. This appears to be envisaging a decentralised App Review and the risk that you identify there, and what I am putting to you is that that risk would not eventuate in the hypothetical world that we are considering where there is centralised Apple App Review of all apps?

A. The risk that it would become more fruitful, is that what you are asking me? Or the risk that there would be fraudulent developers?

Q. What I am putting to you is that the risk that you identify, which is of a legitimate developer seeking -- sorry, of a malicious developer seeking to impersonate

a legitimate developer, does not arise in circumstances where you continue to have full App Review of all iOS Apps by Apple?

A. I think that risk still exists.

Q. But the risk would be no greater than it is in the present day where Apple vets all developers and reviews all apps?

A. Correct.

Q. First Rubin, para 158 {C3/2/81}. If we pick it up in the third sentence, can you see the sentence starting, "In particular ..."?

A. Yes.

Q. You say:

"... there are numerous security benefits associated with using updated versions of Apple's iOS SDK, which is only distributed through Apple."

Yes?

A. Yes.

Q. Then the first benefit you identify is:

"... to download the SDK, each developer must first be registered with a valid Apple Developer Program identity."

Yes?

A. Yes.

Q. We have just been discussing that, and I think you

accepted that in the counterfactual world we are considering, you could continue to have mandatory developer verification, yes?

A. Yes.

Q. So that particular benefit would continue to exist in our counterfactual world, yes?

A. Yes.

Q. If we go over the page, {C3/2/892}, after the word "above", you will see "Second".

Have you got that?

A. I am sorry, I did not know you were waiting for me. Yes. I am there.

Q. "Second, Apple's centralised SDK distribution ensures that Apple Developers are always able to acquire the most up to date SDK versions issued by Apple."

Yes?

A. Yes.

Q. You are addressing here centralised distribution of the SDK, correct?

A. Yes.

Q. That has nothing to do with centralised distribution of iOS Apps, correct?

A. That is right.

Q. Down two lines:

"Third, by having a centralised distribution

channel, it is easier for Apple's latest SDK updates and bug fixes to be communicated to Apple Developers."

Yes?

A. Yes.

Q. Again, you are addressing here a centralised distribution channel for the SDK updates and bug fixes, yes?

A. Yes.

Q. That too has nothing to do with the centralised distribution of iOS Apps, correct?

A. That is correct.

Q. "Fourth, Apple can provide technical support for developers using the official iOS SDK."

A. Yes.

Q. Apple's ability to provide technical support to developers using their SDK does not depend on whether a distribution of iOS Apps is centralised or not, correct?

A. That is right.

Q. If we read on, we see, it is the penultimate sentence:

"In the past, there have been malicious apps associated with the use of infected third-party SDKs obtained through illegitimate channels. Further, there have been third-party SDKs associated with specific functionality that have violated Apple's policies."

Yes?

A. Right.
Q. Here you are referring to SDKs that developers might use in their apps which are not provided by Apple, correct?
A. Right.
Q. Identifying SDKs associated with malicious apps is one of the things that App Review seeks to do, yes?
A. I did not hear you at the end.
Q. I am so sorry. Identifying SDKs associated with malicious apps is one of the things that App Review seeks to do, yes?
A. Yes.
Q. So this is not distinct from App Review, correct?
A. Correct.
Q. If we could go to the article that you refer to in footnote 177, which is at {D2/537/1}, and it is tab 30 of your hard copy bundle, Professor Rubin. You will see it is an article from The Verge.
A. Okay.
Q. Dated 11 December 2020. If we go to page {D2/537/2}, we will see near the top of the page:
"X-Mode works by giving developers code to put into their apps, known as an SDK, which tracks users' location and then sends that data to X-Mode, which sells it."
Yes?

A. Yes.
Q. Next paragraph:
"Apple is giving developers two weeks to remove the SDK ..."
Yes?
A. Yes.
Q. So this concerns an SDK that was in apps that were available on the Apple App Store, yes?
A. That is what it sounds like.
Q. Those apps would necessarily have gone through Apple App Review, yes?
A. Yes.
Q. This is an example of a privacy issue which was missed by Apple's App Review, yes?
A. Yes.
Q. Dr Rubin, you have suggested in your reports that decentralised distribution of iOS Apps would lead to fragmentation of that information, yes?
A. Yes.
Q. You identify two consequences of this. The first is the reduced effectiveness of Apple's App Review?
A. Yes.
Q. The second is a greater burden on iOS device users to make decisions about where to download apps from, yes?
A. Yes.

Q. Let us start with the reduced effectiveness of App Review, okay?
A. Okay.
Q. You say that Apple's App Review would be less effective because information about apps would be fragmented between different parties, yes?
A. Yes.
Q. If all apps, all iOS Apps distributed in the United Kingdom were subject to full Apple App Review prior to distribution from any source, Apple would remain a repository for all information gained during App Review, yes?
A. Gained during the App Review process, but there are other inputs that feed into it that Apple would lose.
Q. I am going to come on to the other inputs.
A. Okay.
Q. But at the initial stage, no fragmentation, because Apple continues to be a centralised repository for information, yes?
A. Can we go back to the last question. I may have misunderstood.
Q. Yes. If all iOS Apps distributed in the United Kingdom were subject to full App Review prior to distribution from any source, Apple would remain a repository for all information gained during App Review, correct?

A. Okay, yes.
Q. In terms of any review carried out by a third-party store, all iOS Apps would have already been subject to static analysis by Apple?
A. Yes.
Q. Dynamic analysis by Apple?
A. Yes.
Q. Human review against the full set of Apple App Review guidelines?
A. If that is your counterfactual, then, yes.
Q. So any review by the third-party would be additional to Apple's App Review, yes?
A. Right.
Q. The only information that would be available to the third-party app store, which was not available to Apple, would be any marketing materials the developer presented to the third-party store, yes?
A. Well, also reviews that were posted by users.
Q. We are going to come on to reviews.
A. Sure, but I just did not want to leave it out.
Q. Of course not, but we will get there.
In terms of marketing materials, Apple would have any marketing materials and presentation for the App Store, yes?
A. Yes.

Q. The third-party store would be able to review the marketing materials, review the app itself, and determine whether the marketing materials were misleading or inaccurate?
A. They could do that if they had the capability. If they had the tools, the resources and the reviewers then that is something that they could do.
Q. They could compare how the app looks and functions and they could compare the written information that was going to go on their site, yes?
A. Assuming they have the incentive and resources to do it then they could do it.
Q. The third-party would have all the information it requires to make that assessment?
A. They could have that if they kept it.
Q. So in terms of App Review, the fragmentation of information only relates to information about apps after they have been through the initial App Review, yes?
A. Well, the initial App Review would be affected by the fragmentation, but otherwise you are right.
Q. Professor Rubin, we have agreed that Apple remains a repository for all information gained during App Review, yes?
A. Right, but there is information gained at other times as well.

Q. But the other times are necessarily after App Review. We have agreed that during App Review, Apple still has everything, yes?

A. Right. I just want to make the point that when App Review is happening, App Review takes advantage of Apple's knowledge base, of all of their information that they have collected. Machine learning depends on that. So if they lose other signals that they might have gotten based on the post-distribution of the app, they will not be able to factor that into their App Review analysis.

Q. We are going to come on to post-distribution. It is just going to help me, and hopefully help the Tribunal, if we go in chronological order.

I understand you say there is a feedback loop, but let us work through chronologically and we can come back to the feedback loop, okay?

A. Okay.

Q. So let us turn then to post-approval detection and removal, okay?

A. Okay.

Q. You make a number of points about post-approval detection and removal across both reports, and so once again what I have tried to do is I have tried to boil them down to six propositions. I am going to give you

the propositions and you can tell me whether I have got them right, okay?

A. Sounds good.

Q. Proposition 1: Apple may lose its ability to monitor apps for post-distribution malicious behaviour?

A. I agree.

Q. Proposition 2: third-party app distributors may not have the ability or willingness to monitor iOS Apps for post-distribution malicious behaviour?

A. I agree.

Q. Proposition 3: third-party app distributors may not inform Apple if they detect malicious apps post-distribution?

A. I agree.

Q. Proposition 4: Apple may not be able to identify apps that are similar to apps that are identified post-distribution which are malicious?

A. I agree.

Q. Proposition 5: Apple may not be able to prevent further distribution of malicious apps detected post-distribution?

A. Agreed.

Q. Proposition 6: malicious apps may be re-submitted after they are detected post-distribution?

A. Can I hear that again?

Q. Malicious apps that are detected post-distribution may be re-submitted to Apple or a third-party distributor?
A. They can be.
Q. I have explored these issues with Apple's factual witnesses in cross-examination last week and the week before, so what I am going to do is I am going to set out that factual evidence, and I am going to ask you some questions about your opinion based on that evidence, okay?
A. Okay.
Q. Let us start with proposition 1, which is identification by Apple. In cross-examination, Mr Kosmynka confirmed that Apple would continue to be able to, firstly, use computer tools to monitor all iOS Apps distributed in the United Kingdom for changes in runtime behaviour post-distribution, regardless of distribution source. Okay?
A. Is there any way to put that on the screen, or ...
Q. You do not have a transcript?
A. If it is at one of my tabs, yes, I can go there.
Q. If you can go to Day 5 -- sorry, this is the transcript of these proceedings, obviously. Day 5, page 200, and let us pick it up at line 19.
A. It would just be easier for me, because that was kind of long.

Q. Of course.
A. Thanks.
MR KENNEDY: It should be -- I think we are running into the age-old problem that the pdf and the Opus version do not match, sir. I am not sure it is a problem I can solve on the fly.
I think the best I can do, Professor Rubin, is reread the question to you, okay?
A. Okay.
MR KENNELLY: I am sorry, if he has been asked to confirm or examine evidence given by Mr Kosmynka, he ought to see it on the transcript. That is the only fair way of doing it.
THE CHAIRMAN: Mr Kennedy can put it to him as a hypothetical, can he not? It is convenient that Mr -- it is obviously important what Mr Kosmynka said, but I do not think it is crucial to the premise, is it?
MR KENNELLY: As long as the witness understands what is --
THE CHAIRMAN: It is entirely open to you to show the transcript to the witness and then of course point out the differences. I think that is probably how we are going to have to do it, Mr Kennedy, unless you are able to find it ...
MR KENNEDY: Sir, I think that is probably the best way of doing it. We can perhaps get proper references for

tomorrow. Or, as you suggest, Mr Kennelly can go to them in re-examination if he thinks I have not summarised them --

THE CHAIRMAN: Well, I think if you are putting it to him as being the evidence of Mr Kosmynka, then he is entitled to see the transcript.

MR KENNEDY: Of course, sir.

THE CHAIRMAN: If you put it to him as a hypothetical and say if this was the position, then he can answer that question, can he not?

MR KENNEDY: He can, sir. Let us do it that way.

THE CHAIRMAN: Let us see how you get on, and if you strike a problem with that then we will have a break at some stage and you might be able to ...

MR KENNEDY: We might be able to do it relatively quickly, sir, perhaps in the transcriber's break, but we will do it on a hypothetical basis as you suggest, sir.

Professor Rubin, I would like you to assume that in the counterfactual world that we have been describing, Apple would continue to be able to use the computer tools it currently uses as part of App Review to monitor all iOS Apps distributed in the United Kingdom for changes in runtime behaviour post-distribution regardless of the distribution source, okay?

A. Okay.

Q. That is assumption one. I want you also to assume that Apple would continue to be able to receive information about malicious applications through user reports, developer reports, from within Apple itself, through press reports, through social media, and by monitoring publications from privacy experts, okay?
A. Okay.
Q. I would like you to assume that Apple would not be able to use user reviews if those user reviews were not posted on the App Store?
A. Okay.
Q. I would like you to assume that Apple would not be able to get information about malicious apps through Apple Care or through the Report a Problem flow?
A. Okay.
Q. With respect to user reviews, you accepted in the Australian proceedings that App Store user reviews only have a limited role in ensuring iOS platform security, right?
A. By having a limited role, I mean they are not the only thing.
Q. So what I am going to put to you, on the basis of the assumptions that I have asked you to make, is that in the counterfactual, Apple will continue to be able to monitor for post-distribution malicious app behaviour

through the vast majority of the channels it currently uses?

A. So that may be the most assumptions I have ever been asked to make to answer one question, so I am going to try to answer that, with the caveat that there were a lot of assumptions in there.

I think what you are saying is that if Apple were somehow able to have all of the information from the third-party app stores that they could possibly have, and the same information that Apple normally gets in the centralised App Store post review, then if they only did not have access to reviews and Apple Care and feedback from users, would they still be able to have most of the capability of doing App Review? Was that the question?

That is my understanding of the question, and I do not want to answer it unless that is exactly right.

Q. It is not exactly right. I did not ask you to make any assumptions about third-party app stores providing any information to Apple. I am focusing here on comparing the information that Apple has available to it in the actual world based on the evidence we have seen in these proceedings.

A. In the real world or in the counterfactual?

Q. In the real world.

A. Okay.

Q. I have asked you to assume -- perhaps we will do it this way. I have asked you to assume that two pieces of information are absent in the counterfactual world, okay?
A. Okay.
Q. The first is user reviews --
A. Okay.
Q. -- if they are not on the App Store. The second/third is information coming through Apple Care or the Report a Problem flow.
A. Okay.
Q. So that is the missing information.
A. Okay.
Q. What I put to you is that in the counterfactual world, Apple would continue to be able to monitor for post-distribution malicious app behaviour through the vast majority of the channels it currently uses?
A. I think that depends entirely on the level of cooperation of the third-party app stores.
Q. I have not asked you to make any assumptions about third-party app stores, we are talking about the information that Apple currently gets. I have not asked you to make any assumptions --
A. Okay, I am confused about the counterfactual, because I do not understand how I can assume that you have

third-party distribution, and yet Apple is still getting all of the feedback that it would normally get. So it does seem contradictory to me.

Q. Shall we look at the sources of the feedback --

A. Okay.

Q. -- and work out whether or not they are connected to third-party app stores, yes?

A. Okay.

Q. So I have asked you to assume that Apple's computer tools can look at runtime behaviour of iOS Apps regardless of distribution source?

A. Okay.

Q. I have asked you to assume that users might still email Apple and say: I have a problem with my app?

A. They might or they would necessarily do it?

Q. They might.

A. Okay.

Q. Developers might email Apple and say: this app is malicious.

A. Okay.

Q. Or an employee within Apple itself might email someone in the App Review team and say: I have got this app, I got it from wherever, it is malicious.

A. Okay.

Q. Apple could continue to monitor the press, social

media --

A. Sure.

Q. -- and publications from privacy experts.

A. Sure.

Q. So third-party app stores do not have to do anything for those channels, this is all Apple directed.

A. Right, but you are saying they might, the third-party stores might notify Apple about something, so --

Q. I am sorry to interrupt you. I have not said anything about third-party app stores telling Apple anything at all.

A. Okay. I am really honestly not understanding something here. When you say that somebody might email Apple about a problem, who are you referring to?

Q. Users.

A. Users. Okay. But they might -- this is where my confusion comes -- they might email the third-party --

Q. They might.

A. -- store instead of Apple, in which case Apple would not be getting the same information.

Q. We are talking about possible sources of information. In the actual world, not every user that has a problem with an app emails Apple.

A. Right. But in your counterfactual, they might have emailed Apple, but because they got the app from

a third-party app store, they might email that app store.

Q. Yes.

A. Okay. But I also do not understand what the ultimate question is at the end of all of these assumptions.

Q. I will have another go, okay?

A. Let us try.

Q. Then we will move on.

In the counterfactual world that I have asked you to imagine, Apple will continue to be able to monitor for post-distribution malicious apps through the vast majority of the channels it currently uses?

A. Okay.

Q. Do you agree or not?

A. Do I agree they would be able to do that? I think many of the channels would not be available to them but some of them would be.

Q. Which channels do you say would not be available to them?

A. User reviews, feedback from users that email their third-party app store instead of emailing Apple, and then there is the effect that the feedback loop has on the quality of app reviews, so the quality of app review itself would be degraded.

Q. We are going to come back to the feedback loop.

A. Okay.
Q. So that was Apple's ability to identify malicious behaviour post-distribution.
Now we are moving on to third-party app distributors, okay?
A. Okay.
Q. Again, we are going to do it on the basis of assumptions since my transcript references are off.
I would like you to make two assumptions -- these are not assumptions, they are a proposition of fact. Are you aware that under the decentralised iOS App distribution model that applies under the DMA, alternative app stores in the EU are under a contractual obligation to Apple proactively to seek to identify and take appropriate action against malicious apps?
A. Yes.
Q. I want you to assume that it may be possible for Apple to require developers of alternative app stores in the United Kingdom to report information to Apple about malicious apps or malicious developers they discover on their App Store.
A. Okay.
Q. Based on that one proposition of fact and that one assumption, what I am going to put to you is that in the counterfactual, third-party app stores are likely to

have a legal obligation to monitor for post-distribution malicious app behaviour?

A. I agree with that.

Q. Also to report such behaviour to Apple?

A. I agree with that.

Q. Moving from the counterfactual to the actual. In the actual world, malicious apps are often discovered by third parties who are under no obligation to report those to Apple but who nonetheless do report those issues to Apple, correct?

A. Yes.

Q. There is no reason to think that those third parties would act any differently in the counterfactual world, is there?

A. There is, because it is possible that users are reporting the problems they find with their apps back to Apple because they downloaded the app from Apple, and if they downloaded the app from a third-party, those users might report it to the third-party that they downloaded the app from as opposed to reporting it to Apple.

Q. Any monitoring for post-distribution malicious app behaviour would be incremental to the monitoring that Apple was doing, yes?

A. Yes.

Q. Now, Professor Rubin, you have suggested that other

distributors of iOS Apps may have fewer resources to carry out a post-approval review, yes?

A. Yes.

Q. If I could just ask you to go to Professor Sweeting's report in these proceedings, which is {C3/3/141}, and it should be tab 26 of your bundle. For the EPE, can we go to page 1, just so I can show Professor Rubin what the document is {C3/3/1}.

Professor Sweeting is an economist instructed by Apple in these proceedings, okay?

A. Okay.

Q. If we could pick it up at paragraph 308 {C3/3/141}, you will see a heading, "Likely Scenarios Absent the Distribution Requirements", okay?

A. Okay.

Q. In this section of his report, Professor Sweeting is looking at the counterfactual world from an economic perspective, okay?

A. Okay.

Q. If we go over to 309 {C3/3/142}, pick it up at the second sentence:

"In my view, one reasonably plausible state of the world is one in which a small number (potentially two or three) of larger alternative iOS App transaction platforms exist in addition to the App Store, along with

a fringe of much smaller alternative iOS App transaction platforms."

Yes?

A. You read that right.

Q. Then picking it up at 310:

"It is likely that at least some of the operators of these larger platforms would be existing technology firms, such as Google, Amazon, Microsoft, Facebook and Sony [and so on]."

Yes?

A. Yes.

Q. Companies like those identified by Professor Sweeting are likely to have similar resources to Apple to carry out-post approval review, are they not?

A. Yes.

Q. Moving then to proposition 3, which is the identification of similar apps.

A. Okay.

Q. Again, we will do it on the assumptions basis. I want you to assume that if Apple became aware of malicious apps post-distribution, it could review the App Store and all iOS App submissions past, present and future for similar vulnerabilities and exploits, okay?

A. One more time?

Q. I want you to assume that if Apple became aware of

a malicious app post-distribution, it could review the App Store and all app submissions past, present and future for similar vulnerabilities and exploits?

A. In the current world, in the real world?

Q. In the counterfactual world.

A. In the counterfactual world.

Q. So centralised app review, decentralised distribution?

A. Yes.

Q. Just to pick up two points from your evidence. If Apple continued to review all iOS Apps prior to distribution, and if Apple became aware of a malicious app after it passed App Review, Apple could adjust the App Review process to prevent such apps from being approved in the future, yes?

A. Yes.

Q. It could adjust its custom written malware scanners, yes?

A. Yes.

Q. Proposition 4: removal. We discussed this before, that if Apple became aware of a malicious app following App Review, Apple could remove it from the Apple App Store?

A. Yes.

Q. It could revoke the app signature?

A. Yes.

Q. It could ultimately ban a developer from submitting iOS

Apps in the future, yes?
A. Yes.
Q. Two questions for you, Professor Rubin. If Apple revokes an app signature, that would prevent any new installations of the app from any source of distribution, yes?
A. Yes.
Q. If the signature was revoked, users who had already downloaded the app from any distribution source would be unable to launch the app on their device; is that correct?
A. If they are online at some point after that, yes.
Q. You do not refer to Apple's ability to revoke signatures in this way in either of your reports, do you?
A. I do not recall saying that.
Q. Final proposition, resubmission. If we go to first Rubin, 174. It is {C3/2/91}. If I could just ask you to read that to yourself, Professor Rubin. (Pause)
A. Which paragraph?
Q. 174. (Pause)
A. Okay.
Q. We see towards the end:
"I note that Mr Federighi observed that slight modification and resubmission of malware could occur, explaining that, with apps submitted for notarisation on

macOS ..."

Then you quote from Mr Federighi's statement, yes?

A. Yes.

Q. Could we go to Mr Federighi's statement. It is {B2/3/35}.

It is tab 4 for you of the white bundle, Professor Rubin. Pick it up at paragraph 121.

A. Paragraph 121?

Q. I may have given you a bad reference. If you give me one moment, please. It is 112, page 35. Apologies.

If we could pick it up halfway down, the sentence beginning "In our experience ..." Do you have that?

A. Yes.

Q. "In our experience, when one instance of malware is detected on macOS and blocked at the code-signing level, it is possible for the developer to slightly modify the malicious software and resubmit it again through the notarisation server. Without Human Review, XProtect will not immediately spot the modified malware. Centralised distribution on iOS permits Apple to block not just the old malware, but also new iterations of that malware (identified with the critical assistance of human review)."

Yes?

A. Yes.

Q. So if all iOS Apps distributed in the United Kingdom were subject to full App Review, including human review, the issue identified here by Mr Federighi should not arise, correct?

A. With the caveat about the loss signals affecting the App Review quality.

Q. Professor Rubin, give me one moment to make sure that I have checked off the items on my six propositions and then we will carry on. (Pause)

Professor Rubin, drawing the threads together, I will slightly restate my question in light of being hampered by the transcript: in light of the assumptions I have asked you to make, what I am going to suggest to you is that there will be no material reduction in the identification and removal of malicious apps post-distribution in a counterfactual world?

A. I disagree with that.

Q. Professor Rubin, the second consequence that you identify from fragmentation of information is a reduction in users' ability to choose between apps from different distribution sources, yes?

A. Right.

Q. If we could pick it up at first Rubin, para 255, which is {C3/2/133}. Have you got that?

A. Okay.

Q. "First, the general user population may lack the security and privacy-oriented technical understanding - and the incentive to gain such understanding - needed to make well-founded decisions regarding security and privacy."

Yes?

A. Yes.

Q. What I want to do is I want to have a look at the document you cite at footnote 318, it is a document called the New Landscape of Digital Literacy. It is at {D1/870.1}, and for you, Professor Rubin, it is tab 13 of the white bundle, okay?

A. Okay.

Q. You see the cover there?

A. I do.

Q. Have you read this document before?

A. Yes.

Q. On page 2 you will see the capsule summary. {D1/870.1/2}. If we pick it up in the third sentence:

"This report uses data from a rigorously designed international assessment to analyse workers' current level of digital skills."

Do you see that?

A. Yes.

Q. So this report is not concerned with the general user

population of iOS device users, is it?

A. That is not the listed population for this article.

Q. I will ask you to take it from me, but there is in fact no mention of the word "security" in this report, is there?

A. This is about digital literacy, which I think is relevant to choosing app stores, which is the context that I quoted it in.

Q. There is, in fact, no mention of the word "privacy" in this report, is there?

A. I do not recall any.

Q. Let us go to para 256 of your first report, so staying on page 133 {C3/2/133}. You see:

"Even when users have some degree of technical sophistication, it can sometimes still be very hard for them to identify that they are under attack, let alone identify the source of the attack, particularly given the increasing sophistication of the attack."

Yes?

A. Yes.

Q. Footnote 322, you cite a paper by Fratantonio et al which describes something they call a cloak and dagger attack. Yes? It is at {C5/197/1}. It is tab 14 for you, Professor Rubin.

A. Okay.

Q. This was an attack that was carried out on the Android platform, correct? You see that from the abstract?
A. Yes.
Q. Again, you see it from the abstract but it exploited certain permissions on the Android platform, yes?
A. Yes.
Q. The first Rubin, 257, pick it up at the start:

"It should also be noted that the belief that a user may choose which store to patronise relies upon the assumption that a user has a realistic choice amongst multiple app stores."

{C3/2/135}.

I would like to show you some more of the economic evidence in this case. If we could go to Dr Singer's report at {C2/8/129}. That is in the next tab for you, Professor Rubin. Dr Singer is an economist instructed by the Class Representative in these proceedings.
A. Okay.
Q. If we pick it up at paragraph 259, which is internal page 129 {C2/8/129}. Pick it up one line down, starting with the word "Moreover ...", you see Dr Singer says:

"... in the counterfactual, presumably most, if not all, iOS Apps would seek to have a presence on the App Store."

Do you see that?

A. Yes.
Q. You are not in a position to disagree with Dr Singer's opinion about what is likely from an economic perspective in the counterfactual?
A. I am not offering economic opinions.
Q. If Dr Singer is correct, iOS Devices would typically have a choice whether to purchase an iOS App from the App Store or from an alternative app store, yes?
A. Your question is if users would have a choice to go to the App Store or to a third-party store?
Q. Yes.
A. I assume that is the case.
Q. Go to second Rubin, paragraph 138, which is {C3/6/62}. We will pick it up in the second sentence:

"Even if an app has been submitted for review under the full set of App Store Review Guidelines, users will still have to bear the burden of risk evaluation at the point where they choose an app for installation. Users must evaluate whether a third-party distribution source is presenting an app accurately, or whether the app's description is intentionally or unintentionally misleading. Attackers can exploit the gap that can be created between the information presented on a third-party distribution source and the app installation sheet displayed on iOS or the other

information that was reviewed by Apple."

Yes?

A. Yes.

Q. The premise in this paragraph is that Apple is conducting full App Review of all iOS Apps regardless of where they are distributed, yes?

A. Yes.

Q. So consistent with the hypothetical that I have been positing for you, yes?

A. Yes.

Q. If a third-party distribution source presented an app in an incorrect -- sorry, an inaccurate or misleading way, they should only be misrepresenting an app that complied with the full App Review guidelines, yes?

A. Either that or one that made it through App Review anyway.

Q. If it made it through App Review anyway, that would be because Apple had failed to identify it as malicious during App Review, yes?

A. Yes.

Q. Let us have a look at what you say about app installation sheets. Pick it up in the next paragraph, it is 139. You say:

"In addition, users could have less information available to them for making this risk evaluation in

a model of multiple distribution sources. For example, the risks of the alternative source posting misleading information, or not checking user-facing information for accuracy or security considerations, cannot be fully avoided even by use of mechanisms, and particularly app installation sheets that Apple introduced in the light of the DMA."

Yes?

A. Yes.

Q. You go on to give a number of reasons about app installation sheets. Let us look at them in turn.

Starting with 140, you say:

"App installation sheets do not necessarily include information equivalent to that on product pages for apps distributed through the App Store, which includes developer identity, other apps from the same developer, rating on the App Store, number of ratings, user reviews, app change history, types of in app purchases and Privacy Nutrition Labels."

Do you see that?

A. Yes.

Q. Footnote 175 is a web page, how to help ensure that you only install apps from the App Store in the European Union. That is at {D2/585/1}, and it is tab 17 for you, Professor Rubin. I will give you a moment to

refamiliarise yourself with that document. (Pause)

A. Okay.

Q. What this document does not set out is the information that is included on the App Store but not included on the app installation sheets, correct?

A. It does not speak about that.

Q. It does not allow us to make the comparison that you posit in that paragraph, correct?

A. That is a form of attack, so I do not think Apple would want to describe an attack in something that they release to the users.

Q. Let us go to para 141. This is the second reason. You say:

"Second, a malicious developer may exploit the other information that users can see about an app on a place controlled by the malicious developer ... For example, when submitting an app to Apple's Notarisation for iOS, an attacker may describe an app as a generic social media app that seeks camera access to--"

A. I am sorry ...

Q. I am sorry?

A. You read the first sentence then you jumped somewhere else, and I ... I was not keeping up with you.

Q. I have skipped down three sentences, I am afraid.

A. Okay. So you went from "malicious developer" to where?

Q. To "For example".
A. Okay.
Okay.
Q. App installation sheets include the app name, yes?
A. Yes.
Q. An app description?
A. Yes.
Q. Screenshots of what the app looked like when it was reviewed by Apple, yes?
A. Yes.
Q. None of that information can be changed by the developer following the notarisation process?
A. Right.
Q. On the hypothetical that we have been considering, so not notarisation for iOS but full App Review, the same process could be followed, yes?
A. Yes.
Q. So if an iOS App was presented as a copycat of a well-known app on a third-party app marketplace but had not been presented that way during App Review, that should be apparent to an iOS device user from a comparison of the app description and the screenshots on the app installation sheet and the information provided on the third-party marketplace, yes?
A. In some instances but I think this is an area where

a clever and tricky developer could actually fool a user, especially non-tech savvy user.

Q. Let us come on to privacy nutrition label. So over the page, 142. {C3/6/64}. You say that Apple will not enforce privacy nutrition labels in the European Union, yes?

A. Correct.

Q. That is a function of the particular regulatory regime under the DMA, yes?

A. Correct.

Q. You noted in paragraph 140 that it was the UK Competition and Markets Authority that asked Apple to make privacy nutrition labels available to users, yes?

A. I am sorry, I did not catch it.

Q. Let us go back to 140 and let us look four lines from the bottom. After footnote 175 you say:

"...Privacy Nutrition Labels, which the UK's Competition and Markets Authority asked Apple to make available to users."

A. Right.

Q. So it is unlikely that in the United Kingdom Apple would not be allowed to enforce Privacy Nutrition Labels, yes?

A. I do not know, that seems like it.

Q. I said we would come on to user reviews. We are there now.

A. Okay.
Q. First Rubin, paragraph 303. {C3/2/157}. I just ask you to --
A. Sorry, I think I am in the wrong ...
Q. Page 157.
A. Okay.
Q. I just ask you to remind yourself of what you said there. (Pause).
A. Okay, I have read it, 303.
Q. Then let us go to second Rubin, 133, and that is {C3/6/59}. This is where you pick up the point about user reviews in your second report or I should say one of the places you pick up user reviews in your second report. (Pause).
A. Okay.
Q. F-Droid is the only example you give of an app distribution source that does not offer user reviews, correct?
A. I do not recall if I have any elsewhere but in this section that is the only example.
Q. I could not find any others. An F-Droid is a catalogue of free and open source software, yes? We get that at {D2/5/11}.
A. Is there a tab for me?
Q. I am so sorry, it is tab 27. Just take that from the

first paragraph.

A. Sure.

Q. This is F-Droid's website if that is not obvious.

A. I am sorry, I forget what the question was.

Q. The question was that F-Droid is a free and open source, a catalogue of free and open source software, yes?

A. Yes.

Q. There are about 3,800 apps in the catalogue. Take that from {D2/510.1} and that is electronic only, Professor Rubin. This is Wikipedia, as you can see. If we can go to page 3, {D2/510.1/3}, we see the heading, "Scope of project".

The F-Droid website lists the apps hosted, over 3,800, and then we see a comparison to the Google Play Store which has about 3 million. Do you see that?

A. Yes.

Q. Would it be fair to say that F-Droid is a pretty niche offering, yes?

A. I think that is right.

Q. Unlikely to be of interest to the more tech savvy Android user, yes?

A. I think so.

Q. The other issue you identify in the paragraphs we have seen in your reports are app distribution sources that offer views but do not monitor those reviews for

accuracy, yes? We can pick it up in 133, {C3/6/59} third sentence:

"A third-party distribution source may not offer reviews or monitor them for accuracy."

Yes?

A. Right.

Q. But you do not give a real world example of an app distribution source that offers reviews but does not monitor them for accuracy, correct?

A. I do not see one here.

MR KENNEDY: Sir, that might be a convenient moment. I am about to move on to my last topic, last topic on distribution. We are on track to finish distribution today I think.

THE CHAIRMAN: Good, we will take a ten-minute break.

(3.08 pm)

(A short break)

(3.21 pm)

MR KENNELLY: Final topic on distribution, Professor Rubin. I want to look at the comparisons you draw between iOS and other platforms, so Android, Windows and Mac, okay?

A. Okay.

Q. Let us pick it up in your first report, page 101. {C3/2/101}.

A. Okay.

Q. You will see the heading "Android, with Sideloading and Less Stringent App Review, Is Less Secure Than iOS", yes?
A. Yes.
Q. In this section of your first report, you set out your opinion on how Android compares to iOS in terms of security, yes?
A. Yes.
Q. In your first report, you identify a number of differences between app distribution on iOS and app distribution on Android, yes?
A. Yes.
Q. I want to look at them in turn. If we could pick it up, next paragraph, paragraph 195, you say:
"However, unlike iOS, Android permits the installation of apps from multiple sources, including third-party marketplaces, sideloading, and preloading by OEMs."
Yes?
A. Yes.
Q. So that is the first difference. That is decentralised distribution, yes?
A. Yes.
Q. If you go to paragraph 201 of your first report, {C3/2/104} and pick it up at the first sentence:

"Apps that are sideloaded on to an Android device may undergo limited to no app review at all ..."

You say:

"... and, for this reason, could contain any manner of malware or spyware."

Yes?

A. Yes.

Q. So if an Android app is downloaded from a non-Google Play Store app store, or from a website, the app may or may not have been reviewed for security issues depending on the source, yes?

A. Correct.

Q. Then you say:

"Android also maintains fewer authorisation mechanisms."

A. Where is that?

Q. I have a bad reference Professor Rubin. If you give me one moment I will find it for you. Give me one moment and I will find the reference. (Pause)

Sorry, Professor, it is back to 195. That is my mistake. It is the next sentence, it is just the next sentence of a different paragraph.

You see:

"Android also maintains fewer authorisation mechanisms; it does not, for example, requires apps to

be signed with ..."

Sorry, for the EPE, could we go back to 195 which starts on 101, please. {C3/2/101} It is the second sentence.

Have you got that, Professor Rubin?

A. Yes.

Q. "... fewer authorisation ..."

Picking it up:

"... certificates obtained from Google or another principal certificate authority."

That is a reference to code signing, yes?

A. Right.

Q. Code signing is an important part of Apple's defence in depth approach to security, yes?

A. Yes.

Q. If we go to paragraph 198, that is page {C3/2/103}, we see the second sentence:

"... developer identities associated with sideloaded apps are not checked so that there is no deterrence for malicious Android app distribution via sideloading."

Yes?

A. Right.

Q. This is a reference to developer registration, yes?

A. Yes.

Q. Developer registration is also an important part of

Apple's defence in depth approach to security, yes?

A. Yes.

Q. Then para 200, you say -- sorry, it is page {C3/2/104}, you say:

"These design choices presented above stand in stark contrast to Apple's App Review and centralised app distribution security layers, which are discussed below. In my opinion, these differences are likely to be a key reason why there are significantly more infections in Android than in iOS."

Yes?

A. Yes.

Q. By "these differences", you are referring to decentralised app distribution, absence of mandatory app review, absence of code signing and absence of developer registration, yes?

A. Yes.

Q. You attribute the higher number of malware infections on Android as compared to iOS to the combined effect of these differences, yes?

A. Yes.

Q. Not solely to the decentralised app distribution model in Android?

A. Right.

Q. There is a further difference between Android devices

and iOS Devices that you do not mention in your report and that is that Android devices are manufactured by multiple OEMs, yes?

A. That is true.

Q. As a result of the fact that Android devices are manufactured by multiple OEMs, there is more inconsistency in the frequency and the timing of security updates on Android devices as compared to iOS Devices, yes?

A. Yes.

Q. This is also a material contributing factor for the difference in security between iOS and Android, yes?

A. Yes.

Q. Professor Rubin, your reliance on third-party analyses of security as between Android and iOS, I want to have a look at those now. Let us pick it up in first Rubin, para 180, which is back on page 94, just so we see ... {C3/2/94}.

Introducing those third-party analyses, you say:

"In order to compare the security benefits enjoyed by iOS Devices and their users, I have first considered available third-party analysis on the security threats experienced by other mobile devices.

"In my opinion, the evidence shows that non-iOS mobile devices historically have been the victims of

malware far more often than iOS Devices and this suggests that a significant reason for that is the fact that these non-iOS mobile devices run operating systems that do not use the centralised app distribution model."

Yes?

A. Yes.

Q. With respect to Android, you rely on two third-party analyses. You rely on the Nokia Threat Intelligence Reports, yes?

A. Yes.

Q. You rely on the RiskIQ study?

A. Yes.

Q. Let us start with RiskIQ, {D1/806/1}, and it should be in tab 65 for you, Professor Rubin.

A. Okay.

Q. "2020 Mobile App Threat Landscape Report" from RiskIQ, yes?

A. Yes.

Q. Let us pick it up on page {D1/806/6}. You see a bar chart, yes?

A. Yes.

Q. Heading:

"The most prolific stores of blacklisted apps in 2020 were ..."

Then we see number 1 was Google, which is the

Google Play Store, yes?

A. Yes.

Q. Number 2, I think it is Xiaomi. 3, APK20. 4, Pconline. 5, Tencent, yes?

A. Yes.

Q. So this bar chart shows that the first party Android App Store, which is the Google Play Store, has the greatest number of blacklisted apps, yes?

A. Yes.

Q. Decentralised distribution cannot account for the high incidence of blacklisted apps on the Google Play Store, can it?

A. No.

Q. The Google Play Store is or would be the centralised distribution point on Android if Android were centralised, yes?

A. I mean, that is kind of a tricky question. I think that Android is not centralised. The Google Play Store is Google's primary App Store, but some of the security problems that I talk about in this case have to do with the existence of a fragmented distribution environment like there is in Android.

Q. We will come on to that, but it is fair to say that Google Play Store is the first party store on Android, yes?

A. Yes.
Q. As you say, some other factor must therefore explain the high incidence of blacklisted apps on the Play Store, yes?
A. Some other factor?
Q. Other than decentralised distribution.
A. No, I think that does contribute to it, the fact that there even exists multiple distribution points, and that it is not a centralised distribution is a factor.
Q. And let's look at the next section at page 6:

"Some app stores are more dangerous than others and have a higher concentration of malicious apps. In 2020, these were the stores from which you were most likely to download a malicious app."

We see Xiaomi, Baidu, Pconline, AppLenovo and APK20, yes?
A. Yes.
Q. There is some overlap with the bar chart that we just looked at, but no mention of the Google Play Store in the list, correct?
A. Correct.
Q. There is no explanation in this document, or no clear explanation in this document as to why these five app stores are the app stores from which you are most likely to download a malicious app, correct?

A. I do not think they give an analysis, it is just measurements.

Q. If we go to {C5/246/1}. This is electronic only, Professor Rubin, so it will come up on your screen. This is a document that Dr Lee was shown yesterday. Do you recall that?

A. Yes.

Q. It is a study that looked at where unwanted apps on Android had been downloaded from, yes? If we could pick it up on page {C5/246/2} and if we could zoom in on the paragraph on the left-hand side that says "Then we examine ..." I just want to pick up, it is four lines from the bottom, five lines from the bottom:

"To compare distribution vectors, we compute their vector detection ratio (VDR), ie the ratio of unwanted apps installed through that vector over all apps installed through that vector."

Yes?

A. Yes.

Q. So that is the definition of VDR.

A. Yes.

Q. If we go to the first bullet, we see Google Player is responsible for 87% of all installs and 87% of unwanted installs but has a VDR of 0.6, yes?

A. You said 87 twice, the second one is 67, but otherwise.

Q. I misspoke, thank you. 87 and 67 is what I should have said.
A. Yes.
Q. If we look at the second bullet, we see:
"... alternative markets are the largest, being responsible for 5.7% of all installs and 10.4% of unwanted installs. However, on average they are five times riskier (3.2% VDR) than the Play market (0.6%)."
That should say VDR, yes?
A. Yes.
Q. So this document explains, I think, why Google Play does not appear in the second list that we saw on page 6 of the RiskIQ document, yes?
A. This is consistent with that.
Q. This document also highlights the importance of not comparing absolute numbers or rates of malware incidents, yes?
A. They take a relative approach.
Q. It is always necessary to consider how a given figure for malware relates to the total relevant population of apps or devices, yes?
A. I think that is a useful tool.
Q. Let us go then to the Nokia Threat Intelligence Report. Let us go to {D1/1473} and start at page 1. It is tab 21 for you, Professor Rubin. This is the 2023

report. You will be more than familiar with it?

A. I am.

Q. If we could pick it up at page {D1/1473/10}, what we see is -- are you at page 10?

"This section of the report provides a view of malware activity in fixed broadband and mobile networks around the world in 2022 and the first quarter of 2023. The data has been aggregated from CSP networks where Nokia NetGuard Endpoint Security solution is deployed. This network-based malware detection solution enables Nokia customers to monitor their networks for evidence of malware infections in consumer and enterprise endpoint devices, including mobile phones, laptops, personal computers, tablets and IOT devices. It is deployed in major fixed and mobile networks around the world, monitoring network traffic for more than 200 million devices."

Do you see that?

A. Yes.

Q. The NetGuard Endpoint Security solution is technology that Nokia provides to communications services providers, yes?

A. Yes.

Q. Communications services providers would include mobile operators and internet service providers, yes?

A. Yes.
Q. Do you know if Nokia provides NetGuard Endpoint Security to mobile network operators in the United Kingdom?
A. I do not know that.
Q. Do you know if Nokia provides NetGuard Endpoint Security to internet service providers in the United Kingdom?
A. I do not know that either.
Q. So you do not know whether any of the data in the Nokia 2023 report relates to users of mobile devices and other devices in the United Kingdom?
A. I do not know.
Q. We see that the technology in question is deployed in major fixed and mobile networks around the world, monitoring traffic for more than 200 million devices. Do you know what proportion of the 200 million devices referred to here are Android devices?
A. (Pause). Can I please hear the first part of that question?
Q. Do you know what proportion of the 200 million devices referred to here are Android devices?
A. I would assume that it is the same distribution as found in the normal internet population but I do not know what that number is.
Q. You would agree with me that in order meaningfully to compare the incidence of malware between different types

of device, what we are interested in is, for example, what proportion of Android devices are infected with malware and what proportion of iOS Devices are infected with malware, not simply what percentage of the total number of devices infected with malware were Android devices or Apple devices?

A. I think both of those are instructive.

Q. Worldwide, there are significantly more Android devices than iOS Devices, yes?

A. Yes, I believe Dr Lee said there were twice as many.

Q. In the Nokia 2021 report, page 18, it is {D1/1044/18}, tab 22 for you, Professor Rubin, you see the middle column, "Secure Mobile App Distribution". You see:

"As of July 2021, Android devices --"

A. I am sorry, what page?

Q. Page 18. It is the last page in the hard copy.

A. Okay.

Q. Middle column, near the bottom, "Secure Mobile App Distribution" in blue?

A. Yes.

Q. "As of July 2021, Android devices accounted for 72.21% of all mobile device. IOS devices accounted for 26.92."

Yes?

A. Right.

Q. So that is the figure given in 2021 by Nokia. So all else equal, you would expect more malware in absolute terms to be detected on Android devices than on iOS Devices, yes?
A. With all things being equal, a little over twice as much.
Q. So the fact that the Nokia reports find more malware associated with Android devices than iOS Devices is, at least in part, simply because there are significantly more Android devices, yes?
A. That accounts for a factor of two, but the study found a lot more than that.
Q. Go to para 186 of your first report. That is {C3/2/96}.
A. Okay.
Q. You see the report, and this is a reference to the --
A. Which paragraph?
Q. 186.
A. Okay.
Q. You see that footnote 219 is referring to the Nokia Threat Intelligence Report, 2023, yes?
A. I am sorry, I cannot hear you.
Q. I am sorry. Paragraph 185, so just looking above.
A. Okay.
Q. We see that footnote 219 is a reference to the 2023 Nokia Threat Intelligence Report, yes?

A. What I heard was you said figure 2.9, but I know that is not what you said.
Q. Footnote 219.
A. Footnote, okay. Yes.
Q. So that is the 2023 report. So the report that is referred to in para 186 at the start appears to be referring back to the 2023 report; is that right?
A. Yes.
Q. If we could go back to the 2023 report -- sorry, shall we read 186:

"The report attributes the greater percentage of Android device infections to the fact that Android permits the distribution of apps from just about anywhere, which refers to the fact that Android devices can download apps from not only third-party marketplaces but anywhere with an app's APK".

Yes?

A. Yes.
Q. If we just go back to the report itself to look at the reasons identified, it is {D1/1473/15}. Let us pick it up at 15. It is tab 21 for you, Professor Rubin. You see the heading "Android Malware", yes?
A. Yes.
Q. You see:

"Android-based devices are not inherently insecure.

However, most smartphone malware is distributed as Trojanised applications and since Android users can load applications from just about anywhere, it is much easier to trick them into installing applications that are infected with malware."

Yes?

A. Yes.

Q. That is where you are picking up that quote, yes?

A. Yes.

Q. "Android users can protect themselves by only installing applications from secure app stores like Google Play and installing a mobile anti-virus product on their device."

Yes?

A. Yes.

Q. Apps distributed through the Google Play store are subject to a combination of human and computer review, yes?

A. Yes. I do not know that Google reviews every single app by human review but a lot of them are.

Q. Some are, yes. We have seen that Android apps that are distributed from other sources may not have been subject to the same level of review, yes?

A. Right.

Q. Some may not have been reviewed at all, yes?

A. Yes.

Q. That difference in the extent of app review between Android distribution sources accounts, at least in part, for the relative incidence of malware across Android app stores, yes?
A. That is a factor.
Q. It is your evidence that even the app review carried out by Google on the Google Play Store is of a lesser quality than Apple's App Review?
A. Yes.
Q. So you would agree that one of the reasons that Android devices suffer from more malware than iOS Devices is because of variable quality in app review, yes?
A. Yes.
Q. The suggestion in the Nokia report and in your report that Android devices suffer from more malware because Android users can load applications from just about anywhere is overly simplistic, is it not?
A. It is one of the reasons, it is not the only reason.
Q. Decentralised distribution is not the only reason that contributes to the higher incidence?
A. Right.
Q. The figures given in the 2023 Nokia report do not isolate the number of malware incidents on Android that are referable to the decentralised distribution model, correct?

A. Correct.
Q. The figures given in the 2021 Nokia report likewise do not isolate the number of malware incidents that are referable to the use of a decentralised distribution system?
A. Correct.
Q. The same is true of the 2020 Nokia report?
A. That is right.
Q. Each of the reports just provides an overall figure or overall proportion of malware on Android and an overall figure for iOS, or in some cases no figure for iOS, yes?
A. They drill down a little more but they do not break it out based on applying what percentage for what cause.
Q. So none of the reports says isolate a number attributable to decentralised distribution?
A. Right.
Q. Professor Rubin, you say in your first report that the Android marketplace in China illustrates the real life consequences of fragmentation in app distribution?
A. Correct.
Q. If you go to the joint experts' statement, that is in your black bundle. It is {C4/1/65} for the EPE. It will just take me a moment to get there.
What we are interested in is proposition 1C.iii-8. Do you have that?

A. I am looking at it.

Q. Great. What we see is the proposition is:

"The comparison of iOS to the Android market in China needs to consider the significant contextual differences, such as government interference and the lack of availability of the Google Play Store. Reports on malware and app violations are useful and applicable to the iOS context if they can adequately address the technical factors influencing the security, in particular, the permission of self-signed apps."

Yes?

A. Yes.

Q. We see your response, which is the final column:

"I agree. The fact that Google's Play Store is banned in China, and that Google had little control over the various third-party Android app stores in China precisely contributes to the fact that third-party Android app stores in China are known to host a higher prevalence of malicious apps.

"As an example, Pinduoduo, one of China's most popular shopping apps with more than 750 million active users per month, was found to have distributed malware-embedded apps on Android devices in China. The distribution of malware embedded Pinduoduo app was facilitated by the use of third-party app stores and

direct distribution mechanisms.

"On the other hand, Pinduoduo does not appear to offer the malware-embedded version of its app in a more curated App Store - namely Apple's App Store or, it appears, the Google Play Store, which both has app review in place."

Yes?

A. Yes.

Q. In the absence of the App Distribution Restrictions, the App Store would not be banned in the United Kingdom, would it?

A. Can I hear that again?

Q. In the absence of the app distribution restrictions, the Apple App Store would not be banned in the United Kingdom?

A. So we are talking about a counterfactual?

Q. A counterfactual world.

A. Got it. I assume it would not be.

Q. In the absence of the app distribution restrictions, Apple would continue to control iOS?

A. Yes.

Q. Subject to any relevant laws, it would have control over third-party app stores on iOS, yes?

A. Yes.

Q. In the absence of the app distribution restrictions,

Apple could and would continue to review all iOS Apps and regardless of where they are ultimately distributed, yes?

A. I think that is one of the assumptions that we are making.

Q. That is one of the assumptions. The Chinese Android marketplace bears no resemblance to the counterfactual in this case, does it?

A. You know, it has some resemblance. There are third-party distribution marketplaces and there would be third-party market distributions, but there are differences as well.

Q. The central features that you identified in your response in the JES was the banning of Google Play, that would not apply, or the analogy would not apply to Apple App Store, correct?

A. Right.

Q. The second factor was Google's lack of control over various third-party stores, that does not apply?

A. Right.

Q. The final paragraph looks at Pinduoduo's conduct in more curated app stores, including the App Store and Google Store which have app review, and you have accepted that in the counterfactual world I am positing, there would be app review of all iOS Apps, right?

A. Yes.
Q. Let us move on to Windows. First Rubin, para 208, {C3/2/108}. You see the heading:
"Windows with Limited Oversight on Hardware Security, User Privileges, or App Distribution, is Less Secure Than iOS."
Yes?
A. Yes.
Q. In this section, you set out your view on how Windows compares to iOS in terms of security, yes?
A. Yes.
Q. You say at 208:
"Windows has three main issues which are not present on iOS that hurt its overall security posture."
A. Yes.
Q. Second sentence. Just have a look at each of them in turn.
The first is identified in paragraph 209 and it is the absence of a hardware backed security in Windows 11 -- sorry, the absence of a hardware backed security prior to Windows 11, yes?
A. Right.
Q. You contrast that over the page, {C3/2/109}, with the existence of Secure Enclave in iOS, yes?
A. Yes.

Q. You accepted earlier that Secure Enclave operates independently of centralised app distribution, yes?
A. It does.
Q. Then paragraph 210, the second difference you identify is that Windows allows for installation of software that requires high levels of privilege, yes?
A. Right.
Q. The final sentence of that paragraph, you say:

"Apps installed by users on iOS Devices through Apple's App Store, on the other hand, cannot be executed with elevated privileges."

Yes?
A. Correct.
Q. You say that privileges are:

"... akin to having entitlements for an app running on an iOS device."

Yes?
A. Right.
Q. Entitlements -- and the entitlements used by an iOS App are reviewed as part of the App Review process, yes?
A. Yes.
Q. The third difference is at 211, and it is that users can ignore warnings about potentially malicious software and execute that software, yes?

If we go over the page, {C3/2/110}, 212, picking up

the second sentence:

"... as discussed in the example above, warnings from Microsoft may be ignored by users; on-device security protections on Windows could be bypassed when users run unknown software on Windows devices. But iOS, in contrast to Windows, can do more than warning users that using administrative credentials to run an unknown program could render a computer vulnerable to attack. App Review specifically checks for and will reject apps that maliciously request unnecessary, or unreasonable privileges."

So again, that is a function of App Review, yes?

A. Yes.

Q. We saw earlier, you agreed earlier, that centralised distribution is not necessary to having App Review of every iOS App, yes?

A. You are asking me if I said that you can have App Review of all the apps and then still distribute them in third-party marketplaces? That is possible.

Q. So none of the differences that you identify with respect to Windows relate to centralised app distribution, correct?

A. (Pause). The third one has to do with the fact that users can turn off their systems control over installation of applications that come from unknown

places or different distribution sites, so I think that one does relate.

Q. But we saw on paragraph 12 that what you contrast that with is App Review's control of the permissions that apps can seek, and you say that App Review can reject apps that maliciously request unnecessary or unreasonable privileges, yes?

A. Yes.

Q. So that is the feature of App Review, not centralised distribution, yes?

A. Well, you asked me if any of the Windows controls had anything to do with distribution sites, and I think the Windows one does, but the corresponding iOS defence is not related to centralised or distributed distribution.

Q. So the benefit that arises from the iOS defence, as you describe it, does not relate to centralised distribution but relates to App Review, correct?

A. Yes.

Q. Get back to paragraph 193 of your first report, {C3/2/101}. You say:

"I consider that the results of these third-party studies ..."

That is a reference to the Nokia and RiskIQ documents that we have been looking at.

"... support the conclusion that iOS's layered

defences and particularly its inclusion of the App Review layer and centralised distribution, make iOS a safer and less vulnerable platform than competitor platforms. Below, I go on to explore in greater depth how Android and Windows differ from iOS, in order to see why this might be the case. As I explain below, my opinion is that Windows and Android face greater security issues because they have non-centralised app distribution models [and so on]."

Yes?

A. Yes.

Q. When you refer here to "below", you are referring to paragraphs 208 to 212 of your report which we just looked at, yes?

A. Also the Android section, but for the Windows part, yes.

Q. Just focusing on Windows for the moment, it is the paragraphs we looked at, yes?

A. Yes.

Q. Just staying around 101, 100. If we could just go to paragraph 192, we see the first sentence:

"third-party analyses also demonstrate that the Windows PC platform also experiences more malware infections than iOS. In the 2023 Nokia Threat Intelligence Report, Windows devices account for 11% of infections in all mobile networks from laptops and PCs

receiving a shared network connection through a mobile device. In the same study, Windows devices account for 20% of infections in a broadband network. In Nokia's 2020 study, Windows ... devices accounted for an even higher percentage of infected devices than Android, at 38.92 in 2020 and 23.10 in 2021."

Yes?

A. Yes.

Q. The absence of hardware-backed cryptographic modules prior to Windows 11 would account in part for the higher incidence of malware on Windows devices as compared to iOS Devices, yes?

A. I do not think so. I think the hardware devices are useful for protecting payment information, but I have not looked at whether or not they contribute at all in preventing malware.

Q. The absence of something like a hardware-backed cryptographic module might create an incentive for attackers to target Windows devices, no?

A. Yes.

Q. That might lead to a higher rate of malware in the Windows devices?

A. Fair enough.

Q. The fact that Windows allows the installation of software that requires high levels of privilege might

also account, in part, for the high incidence of malware in Windows as compared to iOS, yes?

A. Yes, for the same reason.

Q. As with the fact that Windows users could ignore warnings about potentially malicious software and execute that software?

A. Yes.

Q. So decentralised distribution is not the only factor that contributes to the higher incidence of malware on Windows devices as compared to iOS Devices, correct?

A. Yes.

Q. The figures in each of the Nokia reports that you refer to in paragraph 192 do not isolate the number of malware incidents that are referable to a decentralised distribution model on Windows, correct?

A. Right, the Nokia reports do not get into that.

Q. Turning away from Windows, Professor Rubin, and on to Macs, I want to start by discussing some of the differences between Mac and iOS security architecture, okay?

Mac has a decentralised app distribution model, yes?

A. Yes.

Q. Sandboxing is not mandatory on Mac devices, correct?

A. I think it comes with it but you can turn it off.

Q. Mac device users can install unsigned apps?

A. Yes.
Q. Mac users can install apps that have not been reviewed by Apple through the notarisation for Mac process?
A. Yes.
Q. Even apps that have been notarised have not been subject to human review?
A. Correct.
Q. Mac users have a higher level of privilege as compared to iOS device users?
A. Yes.
Q. Let us go to first Rubin, 224, which is {C3/2/116}, you see that third-party analyses also demonstrate that the macOS platform --
A. I am sorry, I am not with you.
Q. I am sorry. 224, page 116 of your first report.
A. Okay.
Q. "Third-party analyses also demonstrate that the macOS platform experiences more malware infections than iOS. In the 2023 Nokia Threat Intelligence Report, macOS devices account for 7% of infections in all mobile networks from laptops and PCs receiving a shared network connection through a mobile device. In the same study, macOS devices account for 16% of infections in a broadband network."
Do you see that?

A. Yes.
Q. If we go to paragraph 253 of your second report, sorry to jump around. That is {C3/6/112}.
A. Okay.
Q. We see:

"As I discussed in my May report, not only does macOS have a different threat model than iOS, but it also has a greater infection rate."

Then skip the next sentence:

"In 2021, Nokia reported that Mac devices constituted 9.20% of the infected devices --"

A. I cannot hear you anymore, I am sorry.
Q. I am so sorry. I am just reading the third sentence, beginning "In 2021, Nokia reported ...", yes?
A. Okay, got it.
Q. Then the next sentence is:

"In 2023 ..."

That is another reference to the 2023 Nokia report, yes?

A. Yes.
Q. You would agree with me that the reduced security enjoyed by Mac device users as compared to iOS device users is a product of the combination of the differences in security architectures that we have just discussed?
A. Yes.

Q. It is not solely attributable to Mac's decentralised app distribution model?
A. Right.
Q. The same question about the Nokia reports, this time the 2023 and 2021 reports. Likewise for Mac, they do not isolate the number of malware incidents that are attributable to decentralised distribution, correct?
A. Correct.
Q. Go back to first Rubin, paragraph 241, {C3/2/125}. If we pick it up about two-thirds of the way down, you see a sentence that begins:

"I further consider the experience of macOS to be useful to consider here."

Can I just ask you to read to the end of the paragraph, please. (Pause)

A. Okay.
Q. Could I ask you to familiarise yourself with -- refamiliarise yourself with paragraphs 243-246 so just this section of your report and what you are discussing here. {C3/2/126-127}.
A. So two pages of reading again. I just want to make sure I do not waste your time.
Q. Absolutely.
A. Okay.
Q. Take as much time as you want. It may be very familiar

to you. It may have been a while. (Pause).

A. Okay.

Q. In those paragraphs what you do is you identify differences between notarisation for macOS and App Review for iOS, yes?

A. Yes.

Q. We have been over this but you have accepted that App Review for iOS is separate from centralised distribution for iOS, yes?

You can have App Review for iOS without having centralised app distribution for iOS, yes?

A. You cannot maintain the same level of security in my opinion but it could be done.

Q. So your analysis in this section does not demonstrate that there are security benefits to centralised app distribution which cannot be replicated in other app distribution models?

A. This is not the part of my report that deals with that.

Q. Professor Rubin, one question on enterprise, distribution.

A. Sure.

Q. Ad hoc distribution. If we go to the first Rubin, 226, {C3/2/117}.

A. Okay.

Q. If I can ask you to read 226 to yourself if you have not

already done so. (Pause).

A. Okay.

Q. As we can see from the final sentence of that paragraph:

"In my opinion, consideration of these two distribution options does not demonstrate that Apple's centralised App Review is not needed."

So your analysis in this section is concerned with the security benefits of Apple's App Review, yes?

A. Yes.

Q. That is enterprise. Professor Rubin, that brings us to the end of the distribution section, subject to just two clarificatory questions which I have about the scope of your evidence which I will ask in a second and then, sir, we can consider -- we have a couple of options as to what we do next but I will clarify the scope of your evidence quickly.

First, I just want to understand to confirm that I understand your evidence in relation to issue 2 in the expert list of issues. Issue 2 states -- we can pick it up actually at the back of your report, appendix A. So {C3/2/195}. Hopefully that will come up on the screen for you.

A. Okay.

Q. Issue 2:

"As to sideloading specifically and any other

relevant alternative means of app or app store distribution on iOS Devices what are the security risks, if any, associated with sideloading (or any other relevant alternative means of app or app store distribution)?"

Yes?

A. Yes.

Q. As I understand your evidence, is that the security risks associated with sideloading are the security risks you identify in connection with moving away from a model of centralised app distribution generally?

A. As opposed to what? I am not sure I understand what you are asking.

Q. What I am asking is whether your evidence in relation to issue 2 is simply your evidence in relation to issue 1C essentially, which is: what are the benefits associated with centralised app distribution?

A. We can look at that section but what I recall is offering evidence about the risks that are associated with sideloading in general and also with specific examples from Android.

Q. We can perhaps come back to it in the morning then, Professor Rubin, and I have the same question in respect of issue 3A, which we can see is:

"What are the security risks associated with

permitting the download of other app stores from the app store ..."

It is the same question which is whether this was simply -- your evidence was simply the same as your evidence early on issue 1C?

A. With respect to 3A, I talk about two things. I talk about the security risks of having third-party distribution stores and I talk about the risks of having an app on the device that is a marketplace because that app will result in other apps being downloaded to the device and so that is not something that App Review is capable of reviewing the way it reviews regular apps that are not marketplaces.

Q. Those are the risks that you identify with unreviewed apps generally, yes?

A. Those, what do you mean by those?

Q. You say that one of the risks that is associated with an alternative app store being available on iOS is that App Review would not be able to review the apps within the app store?

A. Right.

Q. The risks that are associated with that putative inability to review the apps within the app store are the same risks with having unreviewed apps coming from any particular source, yes?

A. Well, it has to do with an app having the ability to download content that cannot be reviewed, so you could only continue to review that through the ongoing monitoring process.

Q. But on the hypothesis that we have been discussing at length this afternoon and with centralised App Review of all iOS Apps, that particular risk falls away, yes?

A. I do not think so because we are talking about apps that are going to download other apps, and so all of the App Review that you would normally do on an app to see if it contains malware etc is not possible because the app is a marketplace as opposed to a program that somebody uses.

Q. But all of the apps available on the alternative app store in this hypothesis have also been through Apple's App Review?

A. I see, under the counterfactual, yes.

Q. Under the counterfactual.

A. Yes.

Q. So that risk falls away if you have on this counterfactual hypothesis, you have centralised App Review of all iOS Apps, yes?

A. Unless there is a vulnerability in the marketplace itself which has become a much more powerful app than other apps.

MR KENNELLY: It may be unnecessary but it might be better if my learned friend spelt out that hypothesis again to make sure there is no confusion because various hypotheses have been canvassed, just to make sure the witness understands precisely the hypothesis which is the basis for the question.

MR KENNEDY: I think we can leave it there, sir, and I can come back to it tomorrow if there is any need to.

THE CHAIRMAN: Dr Rubin, I think what counsel is trying to get at is whether you are making any new and different points from the ones that we have discussed today in those issues 2 and 3. So I think --

MR KENNEDY: That is what I am getting at, sir.

THE CHAIRMAN: -- what Mr Kennedy is trying to suggest to you, is there anything we have not talked about that you want to say in relation to these. Now you are not under an obligation to volunteer these. He has to ask you the right questions but he is just trying to get to the bottom -- I think what he is trying to get at is whether when you talk about sideloading that is something which is incrementally different and problematic in the sort of scenarios that Mr Kennedy has been putting to you.

Now, if you want to hear the scenarios again, as Mr Kennelly suggests, I am sure Mr Kennedy can do that but that is the reason you are being asked these

questions. I do not think there is anything -- it is obviously a long day and you are struggling a bit to work out how it fits in but I think that is how it fits in.

A. I am trying to work out. I am just not really sure I understand.

MR KENNEDY: That is precisely it, sir. There is no hidden motive at all. It is simply I was not sure from reading your evidence what you said the relationship between these things were and for my benefit and for the Tribunal's benefit I was trying to clarify that.

A. Sure, sure.

Q. But we can perhaps come back to it tomorrow if there is anything further. I will review what has been said so far and if I have any further questions I will ask you tomorrow, Professor Rubin. Thank you for that.

Sir, that concludes distribution subject to that point.

THE CHAIRMAN: Yes.

MR KENNEDY: So we could either make a start on payments or we could rise, sir, and come back tomorrow at 10.30. I think that we will have time to finish payments tomorrow even if we rise now, but I am in your hands.

THE CHAIRMAN: Subject to anything that Mr Kennelly wants to say about it, what I do not want to do is to find that

anybody feels unnecessarily constrained and 15 minutes may make a difference on Thursday. What is your current estimate about when you will be finished tomorrow morning? Do you have a sense of that?

MR KENNEDY: Somewhere between an hour and a half and two hours, sir.

THE CHAIRMAN: On that basis, Mr Kennelly, do you have any views? I think it is really for you. You have the benefit here because I suppose actually it's, thinking about it, it is probably -- it is for both of you, is it not really, as to whether we --

MR KENNELLY: Indeed. I think in those circumstances although I am sure we would all love to go home Mr Kennedy should probably carry on.

THE CHAIRMAN: That is what I was probably going to say.

MR KENNEDY: I am grateful, sir.

I was going to start, sir, in a short private session. Perhaps it is a convenient thing to do with the final 15 minutes of the day.

THE CHAIRMAN: Yes, do you think you will have to go into private again?

MR KENNEDY: I hope not. There is one possible area where we need to discuss some numbers which might be convenient in private but that is not right at the end of the payments section but it is just a short

self-contained three pages on.

THE CHAIRMAN: Let us do that then. So we will turn off the live stream please and everybody in the room is in the confidentiality room. So we are on a private section and we are able to talk about the things that ...

(4.17 pm)

(Private session)

(4.29 pm)

(The hearing adjourned until Wednesday, 29 January at 10.30 am)

INDEX

1

2

3

4