

<p>1 Wednesday, 15 May 2019</p> <p>2 (10.30 am)</p> <p>3 (In Open Session)</p> <p>4 THE CHAIR: Good morning, everyone. Welcome to Day 3 of</p> <p>5 this public hearing.</p> <p>6 Mr Krishnan?</p> <p>7 MR KRISHNAN: Good morning, chair. We're hearing from Apple</p> <p>8 this morning. Please may the witness be sworn?</p> <p>9 MS MELISSA MARRUS POLINSKY (affirmed)</p> <p>10 Examination by MR KRISHNAN</p> <p>11 MR KRISHNAN: Good morning.</p> <p>12 A. Good morning.</p> <p>13 Q. Could we please have your full name for the inquiry?</p> <p>14 A. Melissa Marrus Polinsky.</p> <p>15 Q. Ms Polinsky, you should have a bundle in front of you,</p> <p>16 you'll find your statement behind tab A1. Please feel</p> <p>17 free to refer to it at any time. You should also find</p> <p>18 behind your statement two documents that I plan to take</p> <p>19 you to. Those documents will also be displayed on the</p> <p>20 screen next to you, so just whichever is easiest for you</p> <p>21 to look at.</p> <p>22 Can I please start with your role in Apple, what is</p> <p>23 your official title with the company?</p> <p>24 A. I'm the director of investigations and child safety.</p> <p>25 Q. You lead the global security investigations and child</p> <p style="text-align: center;">Page 1</p>	<p>1 safety team; is that right?</p> <p>2 A. Correct.</p> <p>3 Q. That team is known as "the ICS team", for short?</p> <p>4 A. Correct.</p> <p>5 Q. You are a former criminal prosecutor; is that correct?</p> <p>6 A. Yes.</p> <p>7 Q. In your time as a prosecutor, did you work on any cases</p> <p>8 about child sexual exploitation?</p> <p>9 A. I did.</p> <p>10 Q. Could you give the inquiry a little bit more detail</p> <p>11 about some of those types of cases?</p> <p>12 A. Absolutely. I worked as a prosecutor, both at the local</p> <p>13 New York District Attorney's Office, as well as at the</p> <p>14 US Attorney's Office, which is at the federal level in</p> <p>15 the United States, and I worked on domestic child sex</p> <p>16 trafficking of children and adults, I worked on child</p> <p>17 pornography cases, child exploitation cases.</p> <p>18 Q. You joined Apple in 2012?</p> <p>19 A. That's correct.</p> <p>20 Q. You worked in various roles concerning both security and</p> <p>21 child safety; is that correct?</p> <p>22 A. Correct.</p> <p>23 Q. In December 2017, you were promoted to your current</p> <p>24 role?</p> <p>25 A. Correct.</p> <p style="text-align: center;">Page 2</p>
<p>1 Q. Where are you based?</p> <p>2 A. In Washington DC.</p> <p>3 Q. Before we discuss what you and your ICS team do, can we</p> <p>4 discuss Apple itself, briefly. It was established in</p> <p>5 1977; is that correct?</p> <p>6 A. Yes.</p> <p>7 Q. In 2.1 of your statement, you describe Apple as being in</p> <p>8 the business of designing, manufacturing and marketing</p> <p>9 three things. So the first being consumer electronics;</p> <p>10 second, software; and, third, services.</p> <p>11 In terms of the first of those categories, we're all</p> <p>12 familiar with some of Apple's products -- iPhones, iPads</p> <p>13 and so on -- but can you help us with what you call</p> <p>14 Apple's software platforms?</p> <p>15 A. So, first, let me start by saying I'm not an engineer,</p> <p>16 so I will do my best to explain. If you have technical</p> <p>17 questions, I'm happy to take those back.</p> <p>18 In terms of our software platforms, we design</p> <p>19 operating systems for each one of our types of devices.</p> <p>20 So, for instance, our mobile devices, like iPhones and</p> <p>21 iPads, run on iOS, which is our operating system that</p> <p>22 allows the device to function. Our computers, our iMacs</p> <p>23 and MacBooks function on macOS, and we obviously have</p> <p>24 our Apple Watch, which functions on watchOS, and then we</p> <p>25 have our Apple TV, which functions on tvOS.</p> <p style="text-align: center;">Page 3</p>	<p>1 Q. Can you help us with the services that Apple provides?</p> <p>2 A. So we offer a variety of services, including the</p> <p>3 App Store, which is a store through which customers can</p> <p>4 access and purchase apps created by developers who are</p> <p>5 not Apple, they are third-party developers. We offer</p> <p>6 services through Apple Music and we offer services such</p> <p>7 as Apple Pay, which enables payment systems at</p> <p>8 retailers. In the US -- I'm not sure if it's in the</p> <p>9 UK -- we offer services such as Apple Pay Cash, where</p> <p>10 you can pay other people who have our device through the</p> <p>11 programme. We also have iCloud, which offers storage,</p> <p>12 cloud service storage, for customers.</p> <p>13 Q. Thank you. We'll return to iCloud and other services in</p> <p>14 a little bit more detail a bit later.</p> <p>15 Apple does not, itself, run a social network; is</p> <p>16 that correct?</p> <p>17 A. Correct.</p> <p>18 Q. But Apple products are, of course, used to access</p> <p>19 various social networks such as Facebook and so on?</p> <p>20 A. They can be, yes.</p> <p>21 Q. Apple does operate some platforms or services, whatever</p> <p>22 the term is, that enable users to communicate with one</p> <p>23 other, such as iMessage, for example?</p> <p>24 A. Correct. We have what we refer to as more peer-to-peer</p> <p>25 communications. These services don't allow people to</p> <p style="text-align: center;">Page 4</p>

<p>1 find and locate strangers, these services connect folks</p> <p>2 who know each other. So you can use iMessage and</p> <p>3 FaceTime, but only if you know the person's identifier</p> <p>4 on that platform.</p> <p>5 Q. Is there any age requirement for using iMessage, for</p> <p>6 a start?</p> <p>7 A. I don't believe so.</p> <p>8 Q. Is that something you would be able to check --</p> <p>9 A. Yes --</p> <p>10 Q. -- with the team and make an inquiry?</p> <p>11 A. -- I will confirm. Thank you.</p> <p>12 Q. Can you tell us a bit about FaceTime?</p> <p>13 A. So FaceTime is a platform that enables video</p> <p>14 communication between customers who know each other and</p> <p>15 have access to -- to the same platform, so who have our</p> <p>16 devices, for example. So if you -- you must have the</p> <p>17 identifier for another person in order to communicate</p> <p>18 with them, that identifier would either be a phone</p> <p>19 number or an email address, and then, if you can input</p> <p>20 that phone number and email address into FaceTime, you</p> <p>21 can then request a video chat with the person. The</p> <p>22 person can accept, or decline. If the person accepts,</p> <p>23 then you can have a video chat exchange.</p> <p>24 Q. Thank you.</p> <p>25 Is there any age requirement for using FaceTime? If</p> <p style="text-align: center;">Page 5</p>	<p>1 you need to go away and check that ...</p> <p>2 A. I need to confirm. I don't believe so, but I'm not</p> <p>3 sure.</p> <p>4 Q. You mentioned iCloud a little bit earlier, can you tell</p> <p>5 us a little bit about iCloud?</p> <p>6 A. So iCloud is a suite of services that we offer customers</p> <p>7 that are sort of cloud-based storage solutions for our</p> <p>8 customers.</p> <p>9 Q. And iCloud mail, what's that?</p> <p>10 A. iCloud mail is our email platform, so @me.com, @mac.com,</p> <p>11 @icloud.com, all of those domains are provided -- at one</p> <p>12 point or another have been provided to our customers who</p> <p>13 sought to use that service to enable email exchanges.</p> <p>14 Q. Can you help the inquiry understand the scale of Apple's</p> <p>15 presence in the UK? For starters, approximately how</p> <p>16 many people use Apple products and services in the UK?</p> <p>17 A. So, worldwide, we have over 1 billion active devices.</p> <p>18 As I mention in my statement, it's a bit hard to say</p> <p>19 exactly how many are in the UK for various reasons, but</p> <p>20 it's fair to say millions and millions.</p> <p>21 Q. Any idea, among those millions and millions of users,</p> <p>22 how many are under 18?</p> <p>23 A. I don't know.</p> <p>24 Q. How many people does Apple employ in the UK?</p> <p>25 Paragraph 2.2 of your statement, if that helps.</p> <p style="text-align: center;">Page 6</p>
<p>1 A. Thank you. 6,500.</p> <p>2 Q. Where in the UK are they based?</p> <p>3 A. So I know we have a variety of retail stores throughout</p> <p>4 the UK which employs a number of employees. We do have</p> <p>5 some offices in London, and I know we have some offices</p> <p>6 in Cork.</p> <p>7 Q. Can we move on to the topic of the work of the ICS team</p> <p>8 that you lead. Where is the team located?</p> <p>9 A. My team is worldwide. I have staff in Cupertino, in</p> <p>10 London, in Germany and various cities in China.</p> <p>11 Q. Is it right that the team -- you describe the team as</p> <p>12 being based in Sunnyvale --</p> <p>13 A. The majority of --</p> <p>14 Q. -- California; is that correct?</p> <p>15 A. I'm sorry, yes, the majority of my employees are.</p> <p>16 Q. The majority are in Sunnyvale?</p> <p>17 A. Correct.</p> <p>18 Q. What would you describe as the remit of the team, what</p> <p>19 responsibilities do they have?</p> <p>20 A. So we are -- we operate within the legal team, so it's</p> <p>21 legal and global security. I employ lawyers, former law</p> <p>22 enforcement officers and other folks with a strong</p> <p>23 security background. The team handles a wide variety of</p> <p>24 issues. In terms of investigations, we investigate</p> <p>25 a wide variety of matters, including when there are</p> <p style="text-align: center;">Page 7</p>	<p>1 questions of child sexual exploitation or other child</p> <p>2 exploitation just more generally. We investigate fraud,</p> <p>3 we investigate IP theft.</p> <p>4 On the child safety side, I do employ a child safety</p> <p>5 counsel, who serves as an attorney for the businesses</p> <p>6 who may come in contact with child security issues.</p> <p>7 Q. How large is the team?</p> <p>8 A. We have approximately 20 employees.</p> <p>9 Q. Can you help us with the make-up of the team, so what</p> <p>10 sort of people work there?</p> <p>11 A. I employ former prosecutors, former law enforcement</p> <p>12 officers, and I have some analysts and employees who</p> <p>13 have other relevant security background.</p> <p>14 Q. Who do you report to as the director of the team?</p> <p>15 A. I report to the senior director of global security, who</p> <p>16 in turn reports to the senior director of global</p> <p>17 security, who in turn reports to the General Counsel.</p> <p>18 Q. Can we narrow the focus to the ICS team's work in</p> <p>19 response to child sexual abuse material that Apple</p> <p>20 finds.</p> <p>21 At 4.1.3 of your statement on page 6, you give</p> <p>22 an example of a way in which such material may come to</p> <p>23 Apple's attention.</p> <p>24 Can you talk us through that example briefly,</p> <p>25 please?</p> <p style="text-align: center;">Page 8</p>

2 (Pages 5 to 8)

<p>1 A. Absolutely. And I will note that this is merely one 2 example. But we -- the App Store employs reviewers and 3 those reviewers are responsible for ensuring that the -- 4 that any app that initially gets on to our App Store and 5 then, subsequently, once it remains on the App Store, 6 any time it is updated, the App Store review team is 7 responsible for ensuring that the apps comply with our 8 regulations around apps. 9 Our regulations are very prescriptive. Among other 10 things, it obviously prohibits child sexual exploitation 11 among other illegal activity. It also prohibits general 12 adult pornography among many other restrictions. 13 So the App Store team will conduct an eyes-on review 14 of every single app that gets submitted to our 15 App Store, again, both upon initial application to the 16 App Store and then any time an app is updated, and for 17 popular apps, that is multiple times a week. 18 Every time there's a review process, the App Store 19 review team will go in, have eyes on, and take a look at 20 the public content. Obviously, we don't have access to 21 private content within an app, it's not our app, but, 22 during the review process, we have worked with the 23 review team to ensure that they are trained on looking 24 for child sexual exploitation material or evidence of 25 child sexual exploitation material, such as chat rooms</p> <p style="text-align: center;">Page 9</p>	<p>1 that are named things that would be suggestive that 2 they're being used for child sexual exploitation. 3 And whenever there is a question about whether or 4 not there might be some child sexual exploitation 5 material within an app, the App Store review team will 6 contact myself or my child safety counsel and we will 7 conduct a review to establish whether or not it is 8 indicative of child sexual exploitation. 9 If we confirm that the material appears to be 10 indicative of child sexual exploitation, we will take 11 a number of different steps, depending on the context. 12 Q. Thank you very much, I'll just pause you there, just 13 take it by stages. 14 So if an app review team member finds material that 15 might fall into that category of child sexual abuse 16 material, they contact you or the Child Safety Counsel? 17 A. Correct. 18 Q. So that we are clear, is it right that the ICS team is 19 responsible for carrying out each and every 20 investigation that Apple initiates into material that 21 might fall into that category? 22 A. Correct. 23 Q. Are all members of the ICS team involved with those -- 24 those investigations? 25 A. No, no, obviously reviewing child sexual exploitation</p> <p style="text-align: center;">Page 10</p>
<p>1 material is something that would be quite traumatic for 2 someone who is -- has not signed up for that, 3 essentially. And I really do rely on the expertise of 4 folks on my team who have worked with this material 5 before, and so, only former prosecutors or law 6 enforcement officers who have experience working with 7 this type of material and who have volunteered to work 8 on these types of cases can handle these cases. 9 Q. Can you help us with how many of those employees fall 10 into that category within the ICS team? 11 A. So my Child Safety Counsel is primary, and then I would 12 say that there's probably about four or five additional 13 people on my team. 14 Q. So, in all, about six members of the ICS team are 15 involved in these sort of investigations? 16 A. Can be involved, yes. I think that's about right. 17 Q. Where are they based, are they based in the US or based 18 around the world? 19 A. So the majority are based in the US. There is one in 20 the UK who -- who has helped. 21 Q. You'll anticipate my next question. You've helped us 22 with Apple's scale, so billions of devices worldwide. 23 In the UK, there are millions of users, you said, 24 a member of the public hearing the evidence might be 25 quite struck by the fact that there are only six</p> <p style="text-align: center;">Page 11</p>	<p>1 employees worldwide who work on these sort of 2 investigations for Apple. 3 What would be your response to a member of the 4 public raising that concern with you? 5 A. So Apple takes a very holistic approach to child safety, 6 and I think it would be wrong to give the impression 7 that the only resources that are dedicated to child 8 safety reside in my team. They'll be incredibly wrong. 9 And, rather, we view our responsibility to protecting 10 children as something that is every employee's 11 responsibility. 12 And so, to give you an example, we have a child -- 13 I'm sorry, we have a supplier responsibility team, now, 14 obviously, one of our main businesses is manufacturing 15 devices. As you mentioned, we're not a social media 16 company, but we do manufacture devices, and we recognise 17 that the manufacturing of our devices can have 18 a tremendous impact on children around the world, 19 particularly in the places where we manufacture and, 20 going even further, the places where our manufacturers 21 source raw materials from, and so our supplier 22 responsibility team, which is not within my team and is 23 not reflected in any of the resources that I've been 24 discussing, has as their mandate, and we work in 25 partnership with them, to identify risks to children in</p> <p style="text-align: center;">Page 12</p>

<p>1 any places where we conduct our business. 2 And Apple takes its responsibility to children and 3 to the folks who work in our supply chain so seriously 4 that we've actually gone further than, I believe, most 5 any other company, in terms of going all the way down to 6 the mining level to investigate the effects that our 7 products can have on children. 8 And as a result of that investigation, we have put 9 in place a programme to support communities in the Congo 10 where the majority of cobalt mining takes place -- and 11 if you don't know, cobalt is essential to the 12 manufacturing of our devices and most -- most 13 technology. So we've put in place relationships with 14 NGOs. We support NGOs that engage in education, that 15 provide resources and that provide whistleblower 16 opportunities to ensure that children are not engaged in 17 mining, which, in artisanal mining, is actually 18 a really, really big problem because many of the 19 communities are incredibly poor. 20 And so, I just give that as an example of the ways 21 in which we take a much more holistic approach to child 22 safety. And so, the resources that are embedded within 23 my team are really a very, very, very small fraction of 24 the resources that we dedicate to child safety. 25 As you mentioned, we are not a social media</p> <p style="text-align: center;">Page 13</p>	<p>1 platform, and so I imagine that, you know, some of the 2 things that you might have heard from social media 3 companies involve the moderation of the community that 4 they've created online, where strangers can meet with 5 strangers, strangers can interact with strangers, 6 strangers can meet other strangers who have similar 7 interests and, if those interests happen to be prurient, 8 to trade images, to groom children and to meet 9 vulnerable people. 10 Since we do not have that type of community, we do 11 not moderate content. And, in fact, our methods of 12 communication tend to be -- or they are private, they 13 are geared towards folks, as I said, who know each other 14 already, we do not facilitate strangers meeting 15 strangers and, given the nature of our private 16 communications, the majority of which are encrypted 17 end-to-end, we do not have the same moderation. 18 Q. Thank you. 19 Just to clarify, though, I understand entirely the 20 point that if one looks at the issue of child safety in 21 general, there are other teams within Apple that address 22 that issue, and I'll give you an opportunity to give 23 some more examples of that later. 24 But in terms of the -- Apple's response specifically 25 to online material that falls within the category this</p> <p style="text-align: center;">Page 14</p>
<p>1 inquiry is concerned about, it's those six employees in 2 the ICS team that are primarily responsible for that; is 3 that fair? 4 A. In terms of investigating? 5 Q. Yes. 6 A. Yes. 7 Q. At 4.1 of your statement, you describe some of the steps 8 that Apple takes when it becomes aware of this sort of 9 material. Could you talk us through those steps briefly 10 please? 4.1, page 5. 11 A. Yes. So when we do become aware of child sexual 12 exploitation material, we -- it depends on the context 13 in which we find it -- if we are in -- we will report to 14 the National Centre for Missing and Exploited Children 15 where we are in possession of the images. As 16 an electronic service provider, we are required to do 17 so. NCMEC, in turn, is our clearing house in the US, 18 they will then refer on to the relevant local law 19 enforcement agency. If we have reason to believe that 20 there is a child who is actually -- who is actively at 21 risk or that there is a contact offender, we will 22 contact local law enforcement. 23 Q. Can you help us with how quickly this occurs? So Apple 24 finds some material, what's the time frame for the steps 25 that are taken?</p> <p style="text-align: center;">Page 15</p>	<p>1 A. It's fairly immediate. Myself and my other 2 investigators are on call. 3 Q. Can you help us with how many investigations the ICS 4 team had in the last year? 5 A. It was approximately 100. 6 Q. Is that just in relation to the UK or is that across the 7 world? 8 A. No, that is worldwide. 9 Q. Worldwide. 10 How does that compare with previous years? 11 A. It's about consistent. 12 Q. Yes. 13 Again, you'll anticipate my next question. Given 14 Apple's scale, millions of users in the UK alone, 15 a member of the public may be quite struck that the ICS 16 team only conducts a hundred investigations a year 17 worldwide into this sort of material. 18 What would be your response to a member of the 19 public raising that kind of concern? 20 A. I think it all depends on who your comparing us to and 21 what your expectations of us are. Again, if you're 22 comparing us to a social media company, of course that 23 is a drop in the bucket, I'm certain, but, again, we do 24 not have public content that we're moderating, and I'm 25 sure that you can imagine that, if there is an image</p> <p style="text-align: center;">Page 16</p>

1 that becomes a meme, for example, on one of these public
 2 platforms that, within hours, if not days, if not weeks,
 3 you can easily have a million reports from that one
 4 image being circulated through a social media company.
 5 We don't have that type of platform, and so we don't
 6 see those forms of communication.
 7 And we don't employ content moderators for that very
 8 reason.
 9 And so, we just do not see that type of activity.
 10 So if you're comparing us against a social media
 11 company, of course our numbers are going to seem tiny.
 12 If you're comparing us to platforms that have encrypted
 13 methods of communication where privacy is a core value
 14 for the company, customers' privacy is a core value
 15 where the company does not sell its customers' data, and
 16 where there is no social media component, I don't know
 17 how we stack up.
 18 Q. Let's return to the subject of encryption and privacy
 19 a little bit later on, but you raise an issue that
 20 I think we need to talk about in a little bit of detail.
 21 Can we briefly talk about the other teams in Apple
 22 that work on the issue of the safety of children
 23 generally, you've given one example of the supplier
 24 responsibility team.
 25 Are there any other examples you want to give,

Page 17

1 a moment, if we can. Just remind us, what is the
 2 App Store, first of all?
 3 **A. Sure. The App Store is Apple's platform on which**
 4 **customers can identify and purchase, or download for**
 5 **free, apps created by third-party developers.**
 6 Q. Can you help us with roughly how many apps are on the
 7 App Store at any one time?
 8 **A. I -- I don't know.**
 9 Q. At 5.6 of your statement, you mention there may be
 10 millions of apps available on the App Store at any one
 11 time; is that a fair estimate?
 12 **A. Yes, that is absolutely fair, but I don't have any more**
 13 **granularity than that.**
 14 Q. Can we focus for now on apps that are developed by third
 15 parties, rather than Apple, in particular. Could you
 16 walk us through the review process for third-party apps?
 17 So let's say I'm a developer, I've an app that I want to
 18 put on the App Store, what happens?
 19 **A. So every app is subject to our developer guidelines.**
 20 **And as I mentioned, our guidelines are some of the**
 21 **strictest in the industry. We prohibit many types of**
 22 **activity on the apps, we also have controls over privacy**
 23 **in the way that data is used, and so, any time an app is**
 24 **submitted to the App Store, before it is ever published**
 25 **on the App Store, it goes through a review process which**

Page 19

1 looking at paragraph 3.6 of your statement?
 2 **A. There are numerous examples. As I said, we take a very**
 3 **holistic approach to child safety, we don't just focus**
 4 **on online child safety, and so, in addition to supplier**
 5 **responsibility, we have resources dedicated throughout**
 6 **Apple, ensuring the security and safety of all of our**
 7 **customers, and then, in particular, children.**
 8 And so, for example, we have dedicated many
 9 resources to developing robust parental controls. We
 10 believe that empowering parents to make good decisions
 11 and help their children make good decisions is
 12 imperative, and so we've dedicated resources throughout
 13 our software platform to developing parental controls.
 14 Our parental controls include the ability to control
 15 the time that a child's device is able to be used, so
 16 a parent can set blackout periods for devices.
 17 Our parental controls --
 18 Q. We'll discuss those in a bit more detail in a second.
 19 **A. Sure.**
 20 And so, in terms of other resources and other areas
 21 in which our employees work on child safety matters, as
 22 I mentioned, our app review team, we've trained the app
 23 review team in terms of what to look for for child
 24 sexual exploitation material.
 25 Q. Let's drill down into the app review team example for

Page 18

1 involves eyes-on review by App Store reviewers.
 2 These App Store reviewers go into the app and look
 3 through the contents of the app and attempt to ensure
 4 that the app is in compliance with our guidelines. Any
 5 time that an app -- I'm sorry, did you have a question?
 6 Q. No, carry on.
 7 **A. Any time an app is updated -- and that can happen**
 8 **because we've updated our software platform; it can**
 9 **happen because an app has identified a bug that it's**
 10 **attempting to fix; that can happen because an app has**
 11 **an additional feature that it would like to add to the**
 12 **app. And, typically, apps are updated quite frequently.**
 13 **As I mentioned, for more popular apps, it can be**
 14 **multiple times a week that apps are updated. Any time**
 15 **it's submitted for update, it goes through that manual**
 16 **review process all over again.**
 17 Q. At paragraph 5.6, you give an example of how an app is
 18 reviewed for child sexual abuse material. Could you
 19 explain that example, please?
 20 **A. In terms of -- so -- so among other things, we have**
 21 **provided to you the App Store and we update a list of**
 22 **key words that we know are commonly used in child sexual**
 23 **exploitation context, and these are you euphemisms, you**
 24 **know, terms that are used by paedophiles, and so we**
 25 **provide those terms and the App Store reviewers will use**

Page 20

<p>1 those terms to search through apps to try and identify 2 platforms, chat groups, things along those lines that 3 may be utilising those terms to subvert controls that 4 the apps may have put in place. 5 Q. What happens if you find material on these apps that 6 gives you concern? 7 A. So just to be clear, I don't conduct the review. 8 Q. Understood. 9 A. But when an App Store reviewer conducts a review and 10 finds something suspicious, they will call myself or my 11 Child Safety Counsel. 12 Q. What results have you had from this review process in 13 terms of child sexual abuse material? 14 A. So, since November, I believe we've -- we've removed one 15 developer entirely from our platform and taken down all 16 of that developer's apps, and I believe that we've 17 removed 17 apps from our platform. 18 Most notably, we actually removed Tumblr and 19 Telegram for -- for hosting inappropriate material and 20 not having sufficient controls on their platforms. We 21 then worked with those platforms to ensure that they had 22 enhanced controls before we allowed them back on our 23 platform. 24 Q. Can you help us with what it was that alerted you to 25 those platforms, as you say, not having sufficient</p> <p style="text-align: center;">Page 21</p>	<p>1 controls? 2 A. There can be a variety of things that would alert us to 3 a platform not having sufficient controls. We do have 4 mechanisms for customers to report inappropriate 5 material or problems with an app, so we do get reports 6 from customers. We get reports from law enforcement, 7 and we actually welcome reports from law enforcement, 8 and we investigate each one of those incredibly 9 thoroughly, or, as I mentioned, our app reviewers may 10 find some suspicious content. 11 Q. What was it about those apps that fell underneath the 12 standard that Apple expected? 13 A. It depends on the app. In certain circumstances, we 14 have seen evidence of child sexual exploitation 15 material, usually photographs, and, in certain 16 instances, we don't actually find child sexual 17 exploitation material, but we find pornography, adult 18 pornography, which is in violation of our terms and 19 conditions. 20 Q. In terms of the platforms that remain on the App Store, 21 is Apple reasonably confident that those apps don't 22 include this type of material or has all the safeguards 23 that Apple regards as necessary? 24 A. So we will only remove apps when we can confirm that 25 there is child sexual exploitation material or some</p> <p style="text-align: center;">Page 22</p>
<p>1 other violation of our guideline. We obviously receive 2 complaints from customers. We are not just going to 3 remove an app because we received a complaint; we seek 4 to verify. There are limitations of our app review 5 process. We don't, for example, have visibility into 6 private communications that may happen on an app or 7 encrypted communications that may happen on an app, so 8 I can't speak to content that may be found in those 9 platforms. 10 For obvious reasons, we cannot, and do not expect 11 ourselves to, review personal private communications on 12 those apps. 13 We also don't -- we may not necessarily view the 14 entirety of the apps, certain apps are enormous, and 15 so -- but -- but whenever we are alerted to a potential 16 issue on an app, we will go and do a very thorough 17 investigation. 18 Q. Those 100 investigations that your team conducts each 19 year, does that include -- include investigations that 20 arise from the App Store review team? 21 A. It does. 22 Q. Can we turn to the subject of parental controls, which 23 you discuss at page 10 or your statement onwards. 24 Firstly, what are parental controls? 25 A. Parental controls are services that we offer to our</p> <p style="text-align: center;">Page 23</p>	<p>1 customers that enable a parent to have better visibility 2 into a child's device and better control over their 3 child's device, and so it requires setting up of 4 a parent-child relationship through iCloud. 5 Through our parental controls we offer parents 6 controls such as the ability to set a time when devices 7 can or cannot be used. 8 We offer parents the ability to choose apps that 9 a child can or cannot download. 10 Visibility into what are the types of apps that 11 a child may be using and the amount of time that a child 12 may be spending on the device. 13 And so we believe that enhancing parents' visibility 14 and control is paramount to enabling parents to carry 15 out their function. 16 Q. Could you talk us through the actual steps that a parent 17 would need to take to install some of these controls 18 on -- on their child's iPhone or iPad, and so on? 19 A. So we actually have a website, apple.com/families, which 20 runs through a tutorial on how to do it. Without my 21 device, I'm afraid, I -- I'm not in the best position to 22 do it. I'm very device-dependent when it comes to 23 running through those things. 24 Q. Understood. 25 Can you help us with how widely these controls are</p> <p style="text-align: center;">Page 24</p>

1 actually used in practice?
 2 **A. I don't know that, I'm sorry.**
 3 Q. Do you know if that is information that Apple has or --
 4 **A. I don't know, but I can look.**
 5 Q. Thank you.
 6 In terms of educating parents and encouraging them
 7 to use these controls, what efforts has Apple made in
 8 that regard?
 9 **A. So again, we -- we do have a website,**
 10 **apple.com/families, which specifically goes through our**
 11 **parental controls in great detail and the steps on how**
 12 **to set it up.**
 13 Q. Is Apple involved in any educational initiatives to
 14 encourage parents more proactively, rather than simply
 15 having a website, if you understand what I mean?
 16 **A. So -- so we do have some education initiatives. Also,**
 17 **first of all, at our retail stores, all of our retail**
 18 **store employees can offer assistance. We have**
 19 **an AppleCare Repair Centre programme where customers can**
 20 **call with any questions that they may have, and both of**
 21 **these sets of people -- our retail store employees and**
 22 **our AppleCare representatives -- are all very familiar**
 23 **with our parental controls and can facilitate and assist**
 24 **any customers looking to set up parental controls.**
 25 **In terms of education initiatives, I can't speak**

Page 25

1 **the team does, it's a very reactive team. We handle --**
 2 **as I mentioned, we handle the investigations, and we**
 3 **provide counsel to business units on child safety**
 4 **matters, and so our budget really reflects use of**
 5 **outside counsel, and use of other third parties that we**
 6 **may need when a given issue arises, and so it really is**
 7 **specific to what issues may arise and what needs may**
 8 **arise.**
 9 **I think in this past year, I would say we have about**
 10 **\$400,000 or \$500,000 that we've spent.**
 11 Q. So roughly a quarter of the budget is spent on online
 12 CSA investigations in particular; is that fair?
 13 **A. I would say in this past year. Again, it's quite**
 14 **dynamic.**
 15 Q. You are able to give the inquiry one further figure
 16 which is at 3.7 of your statement. What is that figure
 17 and what does it relate to?
 18 **A. So -- so we were asked to provide information about**
 19 **monies that were spent on child sexual exploitation and,**
 20 **as I mentioned, it's a very difficult thing for me to**
 21 **calculate, and I chose a very conservative number, that**
 22 **reflects some hardware that we purchased over the last**
 23 **year to support one of our initiatives. This is**
 24 **an incredibly conservative number, it does not at all**
 25 **reflect contractors, employee hours, resources from**

Page 27

1 **specifically to parental controls. I can certainly ask.**
 2 **I'm not sure -- I'm not sure about that.**
 3 Q. Can we talk about the subject of money. Are you able to
 4 tell the inquiry how much Apple spends in a year
 5 specifically in response to online-facilitated child
 6 sexual abuse in particular?
 7 **A. So, as I mentioned, Apple's approach to child safety**
 8 **generally is a holistic one and it's something that is**
 9 **baked into everything that we do. It is very difficult,**
 10 **we don't ring-fence budgets, our approach is we do what**
 11 **we believe is the right thing to do and we will spend**
 12 **all the resources necessary to achieve that outcome.**
 13 **And so it's very difficult for me to provide**
 14 **a budget on what we do to protect children on our**
 15 **platforms.**
 16 Q. Can you help us with the ICS team's budget in a given
 17 year?
 18 **A. So our total operating budget is probably about**
 19 **\$2 million.**
 20 Q. If you were to give an estimate, knowing the time that
 21 the ICS team spends on CSA issues as opposed to its
 22 other priorities -- you mentioned fraud, identity theft
 23 and so forth -- how much of the budget is dedicated
 24 towards online CSA in particular, would you say?
 25 **A. It's a bit hard to say, given the nature of what**

Page 26

1 **other teams that were dedicated.**
 2 **Generally speaking, when we have initiatives around**
 3 **child safety, we involve and use and work with teams all**
 4 **throughout Apple, and so resources get dedicated to our**
 5 **various child safety initiatives from all throughout**
 6 **Apple.**
 7 Q. Just to help us with the actual figure that was spent on
 8 that new hardware you mentioned --
 9 **A. Oh, sorry, I didn't say it. I'm sorry. \$300,000.**
 10 Q. 300,000?
 11 **A. Mm-hm.**
 12 Q. That is for which years?
 13 **A. For the previous year.**
 14 Q. For the previous year. So 2018 and was that also spent
 15 in 2017?
 16 **A. I'm not sure.**
 17 Q. Right. So it's 300K for 2018; is that correct?
 18 **A. Correct. That was spent on a particular set of hardware**
 19 **for a particular purpose.**
 20 Q. Can I turn now to the interaction between Apple and law
 21 enforcement.
 22 Looking at paragraph 8.3 of your statement, what
 23 kinds of requests do law enforcement agencies make of
 24 Apple?
 25 **A. Excuse me one second.**

Page 28

<p>1 Ah, so law enforcement agencies may request from 2 us: preservation of data held in an Apple account; 3 restriction of access to an Apple account; deletion of 4 an Apple account; or various information held by Apple. 5 Q. Can I focus on the fourth of those categories, so 6 various types of information held by Apple. 7 Let's take a scenario where law enforcement suspects 8 a perpetrator of having CSA material on their iPhone. 9 Their iPhone is locked. The perpetrator refuses to give 10 law enforcement the passcode. Can you tell us what 11 assistance Apple is able to give law enforcement in that 12 scenario? 13 A. So again, just to be clear, these are resources not 14 provided by my team. I'm familiar with the assistance 15 that's provided, but it's not my area of expertise, so 16 if you have additional questions that I don't have the 17 answer to, I'm happy to come back to you. 18 Q. Understood. 19 A. So -- so Apple works very closely with law enforcement 20 and we actually pride ourselves on our dialogue that 21 we've built with law enforcement in order to better 22 understand what they actually need when they come to us. 23 In fact, there was a study, I think about a year ago, 24 looking to understand what were the biggest challenges 25 to law enforcement in terms of conducting</p> <p style="text-align: center;">Page 29</p>	<p>1 investigations, and the particular question was, is 2 encryption the biggest hamper to law enforcement? The 3 answer was no; the answer is a lack of information about 4 how to get data and what data was available, was 5 actually the biggest impediment to law enforcement. 6 And as a result of that study, we rolled out a law 7 enforcement training programme across the world and we 8 actually prioritised training law enforcement officers 9 who work on child sexual exploitation or other child 10 safety cases to receive that training. 11 And as part of that training, we discuss, what are 12 the types of data that Apple has available and how can 13 law enforcement officers obtain that data? We then will 14 work with law enforcement, when they do submit a request 15 to us, and particularly if the request involves the 16 wrong account number, or data that may not be available 17 because it doesn't exist in the account, we work with 18 law enforcement to try and figure out what is the need, 19 what is it that they're trying to access, and then to 20 provide whatever data we do have available that might be 21 responsive with the proper service, of course. 22 Q. Understood. 23 If we circle back to the particular example I gave 24 about a suspect's iPhone and law enforcement wanting 25 access to material on that iPhone that they suspect may</p> <p style="text-align: center;">Page 30</p>
<p>1 be evidence of abuse, the iPhone is locked, the suspect 2 refuses to give the passcode to Apple, what happens 3 then? What assistance, if any, can Apple give? 4 A. It depends on what features the customer uses. So one 5 of the things that we might look at is we offer 6 a service where we would preserve a backup of 7 a customer's device, and we offer that service to any 8 customer and that service is intended for, if you lose 9 your device, if you change devices, we retain the keys 10 and the customer retains the keys, the backup is stored 11 in the cloud, and so, if you are changing your device, 12 for example, you can then sort of automatically have 13 content from a prior device populate on your new device. 14 And we're clear that we maintain the keys for that 15 encrypted data as well as the customer, and so, in cases 16 where we -- where a customer has opted for that service, 17 we would actually have content for a device. 18 Q. Could you just hold that, because that's something I'd 19 really like to discuss, the use of iCloud and what 20 happens when there's a backup on the iCloud, but let's 21 just assume that there isn't a backup, so the device is 22 all on the phone. What -- what options does law 23 enforcement have in that scenario? 24 A. So one of our other points of training is more of 25 a forensics course, which is a little bit more</p> <p style="text-align: center;">Page 31</p>	<p>1 technical, but it discusses the Apple ecosystem, and our 2 Apple ecosystem is intended so that your devices work 3 simpatico. So even if you have content on your phone, 4 if you're using your computer, for example, and you back 5 up your device to your computer or you've shared photos 6 and you have that feature enabled on your computer, even 7 on your Apple TV, law enforcement may actually be able 8 to obtain data that's stored on a phone from other 9 devices that -- that may have been connected to -- to 10 that phone. 11 Similarly, if there are pairing certificates, if one 12 device trusts another device, law enforcement may be 13 able to access the underlying device. 14 Q. Understood. Let's assume that none of that applies in 15 a particular circumstance, so we've just got the phone, 16 the suspect doesn't give the iPhone passcode. Is law 17 enforcement simply out of options, at that stage, in 18 terms of assistance from Apple? 19 A. In terms of obtaining -- in terms of the specific 20 question of obtaining the photos, I'm not sure -- again, 21 it's not exactly my area of expertise, so I'm not sure 22 if there would be other avenues available. There's 23 certainly other data that could be available, depending 24 on what's relevant for law enforcement. So we would 25 retain IP address logs, so if -- if location is</p> <p style="text-align: center;">Page 32</p>

<p>1 relevant, we could certainly provide those.</p> <p>2 Again, it really depends on what services the</p> <p>3 customer is using, and I apologise, it is not my area of</p> <p>4 expertise, but I'm happy to go in and research that</p> <p>5 question a little bit further and come back to you.</p> <p>6 Q. Understood. Thank you.</p> <p>7 Could we look at 8.13 of your statement where you</p> <p>8 make a distinction between access to iPhones and so</p> <p>9 forth, depending on what version of iOS a customer is</p> <p>10 using. Could you talk us through that distinction,</p> <p>11 please?</p> <p>12 A. Yes.</p> <p>13 So for devices that are running pre iOS 8, Apple is</p> <p>14 able to extract data from locked devices. Post iOS 8 --</p> <p>15 again, iOS is our operating system -- so post iOS 8, we</p> <p>16 are unable to extract data from a locked device.</p> <p>17 Q. Can you help us with how that change came about, was it</p> <p>18 a conscious decision on Apple's part to change the</p> <p>19 operating system such that access could no longer be</p> <p>20 given to law enforcement --</p> <p>21 A. I can't speak to that.</p> <p>22 Q. -- where a device is locked?</p> <p>23 A. I'm so sorry, I can't speak to that, I don't know.</p> <p>24 Q. Understood. So just help us with some dates as well,</p> <p>25 when was iOS 8 rolled out?</p> <p style="text-align: center;">Page 33</p>	<p>1 A. I don't recall offhand.</p> <p>2 Q. So -- so the position in summary is that, if you're</p> <p>3 running iOS 8 onwards, unless you have these sort of</p> <p>4 back-ups available on iCloud or links with other Apple</p> <p>5 devices, if all the data is on your phone, so to speak,</p> <p>6 law enforcement can't access the data; is that correct?</p> <p>7 A. So again, it depends on what data you're talking about.</p> <p>8 And -- and I -- I don't feel comfortable making that</p> <p>9 assertion, I'd like to go back and ask experts in the</p> <p>10 field on that. But there certainly is data that's</p> <p>11 available, I just don't know the relevance to your</p> <p>12 example.</p> <p>13 But so, for example, certainly online orders, we</p> <p>14 maintain records surrounding online orders. We maintain</p> <p>15 records surrounding purchases made in stores. Any</p> <p>16 records surrounding iTunes purchases, App Store</p> <p>17 purchases, basically transactions that happen through</p> <p>18 our platforms, and so we certainly would likely have</p> <p>19 data, it really depends on the particular example, what</p> <p>20 services a customer has been using. So it's a bit hard</p> <p>21 to answer in the abstract, I apologise.</p> <p>22 Q. Understood. I've received a helpful note saying iOS 8</p> <p>23 was rolled out in late 2014; does that sound about</p> <p>24 right?</p> <p>25 A. Again, I can't speak to it offhand, but if that's what</p> <p style="text-align: center;">Page 34</p>
<p>1 you're saying, I -- it certainly doesn't sound wrong,</p> <p>2 but I don't know, I'm sorry.</p> <p>3 Q. Thank you.</p> <p>4 Leaving that point, can we turn to the use of</p> <p>5 FaceTime.</p> <p>6 What if law enforcement suspects a perpetrator of</p> <p>7 using FaceTime to, for example, live stream the abuse of</p> <p>8 a child? In that scenario, what assistance can Apple</p> <p>9 provide law enforcement?</p> <p>10 A. So again, it depends on what data would be helpful to</p> <p>11 the law enforcement investigation. FaceTime is</p> <p>12 an encrypted platform, it's encrypted end-to-end and we</p> <p>13 don't have the keys, so we do not have the ability to</p> <p>14 view any transactions that are actually occurring</p> <p>15 throughout that live stream. We do maintain records of</p> <p>16 FaceTime invitations, so where, if you, for example,</p> <p>17 invite me to a FaceTime communication, we would see</p> <p>18 a record of that invitation.</p> <p>19 Q. Has Apple provided that sort of information to law</p> <p>20 enforcement on request?</p> <p>21 A. I believe we have. Again, that's not my team, I don't</p> <p>22 provide that data, but my understanding is we have.</p> <p>23 Q. To Apple's knowledge, to what extent is that product in</p> <p>24 particular used -- live stream abuse, does Apple have</p> <p>25 any knowledge about that?</p> <p style="text-align: center;">Page 35</p>	<p>1 A. I don't. Again, FaceTime is different from many other</p> <p>2 video chat platforms, we don't have channels, folks</p> <p>3 can't subscribe to channels or just search for a user</p> <p>4 name. You know, you can't search for "Melissa Polinsky"</p> <p>5 and then figure out what my handle is. So you really</p> <p>6 have to know the person. It's not intended for mass</p> <p>7 groups of people to congregate, you actually have to go</p> <p>8 in and invite people to -- to chat or to video chat.</p> <p>9 And so -- but the answer is I don't know and I would</p> <p>10 imagine it's used -- it's -- it's a difficult platform</p> <p>11 to use if you're looking to engage in activities that</p> <p>12 I've been familiar with as a prosecutor, where you have</p> <p>13 people joining a room of a bunch of different folks then</p> <p>14 paying bit coins to watch various illicit acts.</p> <p>15 Q. Is it possible for someone to use a social media</p> <p>16 platform to meet a stranger and then invite that person</p> <p>17 to go on to FaceTime and thereby use FaceTime to live</p> <p>18 stream abuse.</p> <p>19 A. It's possible, anything is possible, of course, and</p> <p>20 particularly any -- any private communication channel</p> <p>21 can be used, absolutely.</p> <p>22 Q. Is there any -- we've talked about FaceTime invitations</p> <p>23 being data that law enforcement are able to access. In</p> <p>24 Apple's engagement with law enforcement, have law</p> <p>25 enforcement expressed any concern about the use of</p> <p style="text-align: center;">Page 36</p>

1 FaceTime for this sort of abuse?
 2 **A. Not to my knowledge. Not to my knowledge.**
 3 Q. Can I ask you similar questions about iMessage. Just
 4 remind us again what iMessage is?
 5 **A. Absolutely, iMessage is a -- it's akin to text message,**
 6 **it's a platform through which individuals who know each**
 7 **other or know each other's identifiers, such as phone**
 8 **number or iCloud email address, or iCloud address, can**
 9 **communicate through a text message chain, essentially.**
 10 Q. Understood.
 11 And one can assume that the same process could apply
 12 that someone could meet someone on an open social media
 13 network and then the conversation could move on to
 14 iMessage, as it were?
 15 **A. Again, absolutely, any private communication would be**
 16 **vulnerable to the same activity.**
 17 Q. Your evidence was that iMessage was end-to-end
 18 encrypted?
 19 **A. Correct.**
 20 Q. So the same answers apply in terms of law enforcement
 21 access; in other words, law enforcement can't be given
 22 access to iMessage conversations. Is that correct?
 23 **A. So again, it depends on what features the user has --**
 24 **has implemented. If a user has -- has stored back-ups,**
 25 **then contents of iMessages would reside in the back-ups.**

Page 37

1 **All of that data is fundamentally accessible without**
 2 **encryption. Our platforms are under attack constantly**
 3 **by hackers who are looking to obtain whatever data they**
 4 **can obtain.**
 5 **Now, we view it as a fundamental right of our**
 6 **customers, and one of the things that our customers**
 7 **looks to us for is to protect their data in ways that**
 8 **other companies do not, and encryption is really central**
 9 **to that.**
 10 **And as much as I would love to have an exception**
 11 **that would only be an exception for child protection,**
 12 **that would be amazing, the truth of the matter is that**
 13 **any exception to encryption is an exception for anyone**
 14 **and is something that can be exploited by anyone -- by**
 15 **bad actors, by hackers, by various governments around**
 16 **the world for different purposes.**
 17 **So the only way that we can guarantee our customers**
 18 **the privacy and security that they demand of us is**
 19 **through encryption.**
 20 Q. Do you think that Apple has struck the right balance
 21 between the concern to protect users' privacy and other
 22 fundamental rights and interests that are at stake; for
 23 example, the rights and interests of children to be
 24 protected from this kind of abuse?
 25 **A. I do. And part of the reason why I say that is because**

Page 39

1 **If law enforcement is looking to -- for us to**
 2 **intercept iMessages, for example, we cannot do that.**
 3 Q. Has law enforcement expressed any particular concern
 4 with the use of iMessage in this way?
 5 **A. Again, not to my knowledge.**
 6 Q. Now is as good a point as any to grapple with the
 7 subject of encryption.
 8 A reader of your statement could be quite struck by
 9 the prominence that privacy is given in it. For
 10 example, at paragraph 2.4, you say that privacy is
 11 a fundamental human right.
 12 Could you help us with the priority that Apple gives
 13 to privacy?
 14 **A. Absolutely. As I mentioned, we take our customers'**
 15 **privacy and security as paramount. We do not sell our**
 16 **customers' data. We do not -- we seek to protect our**
 17 **customers, we view encryption as being fundamental to**
 18 **the protection of our customers.**
 19 **Without encryption -- I want you to consider the**
 20 **types of data that you may have on any one of your**
 21 **electronic devices: your photographs, your personal**
 22 **photographs; your passwords; your medical records; your**
 23 **financial documents; communications with loved ones;**
 24 **potentially the location of loved ones and/or of your**
 25 **children if you've enabled Find My.**

Page 38

1 **of the way our platform is structured and the resources**
 2 **that we have dedicated to protecting children in all**
 3 **aspects of our supply chain and as -- and part of our**
 4 **customer base.**
 5 Q. Could you help me with that, so you said that "that's
 6 because of the way our platform is structured".
 7 Could you elaborate on that, please? What do you
 8 mean by that?
 9 **A. So, our platform is designed -- as I mentioned, iMessage**
 10 **is encrypted, FaceTime is encrypted, and that's by**
 11 **design. We do not hold the keys for that. And that's**
 12 **in the way it was designed. Does that answer your**
 13 **question?**
 14 Q. So -- but that -- those are structural features that
 15 protect the right to privacy, but those aren't
 16 structural features that necessarily assist in the
 17 protection of children.
 18 **A. I think it depends on what facet of children's**
 19 **protection you're looking at. And, again, I really do**
 20 **wish that there was a way to grant an exception through**
 21 **encryption for a singular purpose, where it would only**
 22 **be used for that singular purpose, but, unfortunately,**
 23 **technologically, my understanding is that that's not**
 24 **possible, that any exception can be abused.**
 25 **What we do protect are: children's communications**

Page 40

<p>1 with their parents; parents' communications with 2 children's doctors and teachers; parents' communications 3 between each other; parents' photographs of their 4 children; children's photographs of themselves. 5 Q. Can we turn now to iCloud, just remind us again what 6 iCloud is? 7 A. iCloud is a service that we offer which involves -- it's 8 our digital storage solution. 9 Q. What kinds of user data are held on iCloud? 10 A. So, again, it depends on what features are used by -- by 11 our customers. iCloud mail, for example, would be 12 stored, could be stored, in iCloud, depending on what 13 data the customer has maintained. 14 Photos, music, downloads, documents, contacts, 15 notes, all of these things might be maintained within 16 an iCloud account, depending on the settings and the use 17 of the customer. 18 Q. Is iCloud encrypted? 19 A. Yes. 20 Q. Can one use iCloud to share images and video? 21 A. Yes. 22 Q. So if law enforcement suspects a perpetrator of using 23 iCloud to do so, what sort of assistance can Apple 24 provide? 25 A. So, again, it depends on what data is available in the</p> <p style="text-align: center;">Page 41</p>	<p>1 account and what services the customer has been using. 2 So my answer would be very similar to my previous 3 answers in terms of back-ups, in terms of customer 4 registrations, customer data, email addresses, phone 5 numbers, IP addresses. 6 Q. Understood. Has law enforcement raised any specific 7 concerns about iCloud being used to either store or to 8 distribute this kind of material? 9 A. Raised any concerns to me? Not to my knowledge. I do 10 know that we do receive search warrants for child sexual 11 exploitation material but, beyond that, I don't know. 12 Q. If we can step back from the detail of the various apps 13 and services, if Apple receives a request for assistance 14 from law enforcement, can you talk us through the next 15 steps? I'm looking in particular at 8.4 of your 16 statement, if that's helpful. 17 A. Thank you. 18 Yes, Apple -- we have a centralised process for 19 tracking, processing and responding to law enforcement 20 requests. Again, that goes through our privacy and law 21 enforcement team, which is not my team, but they are 22 trained on responding to these sorts of requests and, as 23 I said, we really do pride ourselves on the back and 24 forth that we maintain with law enforcement to best 25 understand what it is that they need and what data we</p> <p style="text-align: center;">Page 42</p>
<p>1 might have that might be responsive and helpful to their 2 investigation. 3 Q. Where is that specialised team based, are they in the UK 4 or the US? 5 A. So I know that there's a presence in the US, I believe 6 that there is a presence in Cork, I don't know about in 7 the -- I don't know beyond that. I apologise, it's not 8 my team, I'm not sure exactly where they're 9 geographically located, but I know there's a presence in 10 Cupertino and Cork. 11 Q. Any idea how large that team is? 12 A. I don't. 13 Q. At 8.6 and 8.7 of your statement, you discuss the law 14 that applies to requests by law enforcement for user 15 data. 16 Can you help with where the data of UK-based Apple 17 users are stored? 18 A. I don't know. 19 Q. So you say at 8.6 that user data in the EEA -- the 20 European economic area -- is stored in Ireland; is that 21 correct? 22 A. It says it's controlled by Irish Distribution 23 International in Cork, but I don't know where it's 24 actually stored. I don't know if that means it's 25 stored -- I'm sorry, I'll have to get back to you about</p> <p style="text-align: center;">Page 43</p>	<p>1 that. 2 Q. You say there that requests for user data that is 3 stored -- that is controlled by the Irish entity, is 4 governed by Irish law; is that correct? 5 A. Yes. 6 Q. Do you know the implications of this for access by law 7 enforcement of the specific requirements that Irish law 8 provides? 9 A. I don't know. 10 Q. This may be something out of your -- 11 A. It is, I apologise. 12 Q. Assuming that some data is stored in the US, as you 13 suggest at 8.7, can you help us with the process that 14 must be followed where data is stored in the US? 15 A. Again, not my area of expertise, but I'll answer to the 16 best that I can. 17 Any data that's stored in the US is subject to US 18 law and, for practical purposes, this means that foreign 19 law enforcement will have to go through the MLAT process 20 for any non-exigent data request. 21 Q. Can I pause you there, can you briefly explain what the 22 MLAT process is? 23 A. Absolutely. The MLAT process is, as I understand it, 24 a rather cumbersome process through which law 25 enforcement goes to the US, submits a request for data</p> <p style="text-align: center;">Page 44</p>

<p>1 through the US, the US then processes it and will serve 2 process directly on a company. And so, for our 3 purposes, we wouldn't necessarily know that that request 4 is coming from the UK. Because it's being processed by 5 the Department of Justice. 6 Q. You described it as a "cumbersome process". How so? 7 A. It involves numerous steps for the requesting law 8 enforcement agency and then requires the law enforcement 9 agency to basically come to the US and then have the US 10 serve the process, rather than coming directly. 11 This is why we support the comity provisions of the 12 CLOUD Act. 13 Q. Can you help us -- is there any work-around that's used 14 by UK law enforcement, rather than going through the 15 MLAT process? 16 A. I don't know about work-around, but what I can say is 17 that, for any exigent circumstances, we do accept 18 process directly -- and, actually, not even process, we 19 require -- 20 Q. Sorry exigent circumstances? 21 A. Sorry, so exigencies are any situation -- they're 22 emergencies and we define "emergency" as any situation 23 in which a person or a child is in danger, and so, when 24 we receive a certification from law enforcement that the 25 data that they're requesting is -- meets that criteria,</p> <p style="text-align: center;">Page 45</p>	<p>1 we will provide data directly to that law enforcement 2 agency on an exigency basis. 3 So for the purposes of exigency, child safety, where 4 law enforcement perceives that a child is being 5 endangered, that would meet our criteria for exigency. 6 So we do see, I believe -- again, not my team, but my 7 understanding is that a large portion of our exigent 8 requests relate to child safety matters. 9 Q. Understood. 10 Can you help me, this may be, again, outside your 11 expertise, but is it a matter of US law that, when these 12 sort of exigent circumstances apply, industry players 13 like Apple can provide data voluntarily without having 14 to go through the MLAT process? 15 A. That's my understanding, yes. 16 Q. You mentioned the CLOUD Act before. Can you help us 17 with what the CLOUD Act is all about? 18 A. So particularly, the comity provisions of the CLOUD Act 19 is something that we very strongly support. The comity 20 provisions of the CLOUD Act would enable a foreign 21 government seeking information about their citizen to 22 come directly to a company in the US in order to obtain 23 the data without having to go through the MLAT process. 24 Q. The CLOUD Act has come into force, has it? 25 A. I don't believe it has yet. Am I wrong about that?</p> <p style="text-align: center;">Page 46</p>
<p>1 Q. I'm -- 2 A. I don't believe it has -- 3 Q. It's unclear from the material in the public domain, but 4 that's something certainly we can clarify later. 5 Can you help with the difference that Apple expects 6 the CLOUD Act to make? 7 A. We hope it's easier for law enforcement, quite frankly, 8 to not have to go to through the MLAT process in order 9 to get information about its own citizens. 10 Q. Can you tell us about the time frame for responding to 11 law enforcement. So let's say that Apple receives 12 an MLAT request from the UK or elsewhere, what's the 13 time frame for a response? 14 A. Is there a particular paragraph that you're looking at? 15 Q. 8.8 and 8.9. 16 A. Thank you. 17 So for non-exigent responses, the response time may 18 fluctuate depending on the volume of request and the 19 complexity of the research that we need to do. In 20 practice, responses to standard requests are provided 21 within approximately one week in the majority of cases. 22 For exigent or emergency requests, we respond to them as 23 soon as possible, and we actually have folk, staff, 24/7 24 to intake and process those requests. 25 MR KRISHNAN: Chair, this is a convenient moment for</p> <p style="text-align: center;">Page 47</p>	<p>1 a break, if you're happy with one now? 2 THE CHAIR: Yes, we'll return at 11.55 am. 3 MR KRISHNAN: Thank you, chair. 4 (11.40 am) 5 (A short break) 6 (11.55 am) 7 MR KRISHNAN: Could we just go back on one point just to 8 clarify. 9 Your evidence was that iCloud was encrypted. I'm 10 looking at 8.12 of your statement, in particular. 11 It's right, isn't it, that there are circumstances 12 in which iCloud data can be made available to law 13 enforcement despite the encryption protections that are 14 applied to iCloud data? 15 A. Yes. I don't know if it is turned over to law 16 enforcement in an encrypted state, I need to check. 17 Q. It may help for you to remind yourself of the top of 18 page 16 of your statement, so the last sentence of 8.12. 19 A. Yes, that's for back-ups. So what I say here is that 20 when iOS device back-ups are provided to law enforcement 21 agencies in encrypted form we provide the keys as well. 22 Q. Can you help us with the distinction between Apple's 23 approach there and Apple's approach to peer-to-peer 24 communications of an iMessage, for example, where 25 they're encrypted end-to-end and there's no question of</p> <p style="text-align: center;">Page 48</p>

1 law enforcement having access? So why does Apple make
 2 that distinction?
 3 **A. So in terms of our back-ups, back-ups are a service that**
 4 **are provided to customers. Again -- and we make public**
 5 **that we maintain a key, the customer maintains a key,**
 6 **the idea being that if a customer loses their device or**
 7 **loses access to their device and relies on Apple to**
 8 **provide them with their data, that we're able to provide**
 9 **them with their data. So, given the nature of that**
 10 **service -- and again I'm not an engineer -- but my**
 11 **understanding is that we maintain the keys for that**
 12 **instance. Whereas for FaceTime and iMessage, those are**
 13 **individual communications and we don't maintain the**
 14 **keys.**
 15 Q. Could we turn now to 8.17 of your statement, and could
 16 we have the table put up on the screen, please.
 17 So you describe it as a high level overview of
 18 requests that are made from government and law
 19 enforcement agencies in the UK. You say over the past
 20 five years Apple has received over 15,000.
 21 Do you know how many of these 15,000 requests
 22 related to online facilitated CSA in particular?
 23 **A. I don't.**
 24 Q. Do you know if Apple keeps data of that kind?
 25 **A. I don't.**

Page 49

1 you.
 2 So this is a public document; isn't that correct?
 3 **A. Yes.**
 4 Q. This was published when in 2018, do you happen to know?
 5 **A. I don't.**
 6 Q. Can you help us with when Apple started to publish
 7 reports like this?
 8 **A. I don't know.**
 9 Q. It may be helpful, at 8.14 of your statement I think you
 10 give the date of 2013. 8.14, I apologise.
 11 **A. Yes, 2013, thank you.**
 12 Q. Do you know what brought about the decision to start
 13 publishing these reports?
 14 **A. I don't.**
 15 Q. Can we turn to page 7 of this document, please. Could
 16 we have the whole page first, if you wouldn't mind.
 17 So this is a table of account requests that were
 18 made worldwide. Just remind us briefly what account
 19 requests are.
 20 **A. I believe -- and, again, this is not my document and so**
 21 **I don't want to speak definitively -- but I would**
 22 **imagine that account requests refer to requests related**
 23 **to Apple IDs or iCloud accounts.**
 24 Q. In fact, yes, at the very top of --
 25 **A. Ah yes.**

Page 51

1 Q. Can you help us with the first column of that table.
 2 You'll see the various descriptions, "device requests",
 3 and so forth. Can you help us with what each of those
 4 mean?
 5 **A. So this is, I believe, from our transparency report --**
 6 **and, just to be clear, that's a report that I don't**
 7 **generate, so again not my area of expertise but I'll do**
 8 **my best. So we have "device requests", we have "account**
 9 **requests", so I assume "device requests" refers to**
 10 **information related to devices, whereas "account**
 11 **requests" refers to requests related to iCloud accounts**
 12 **and Apple IDs.**
 13 **"Financial identifier requests", "emergency**
 14 **requests" and then totals.**
 15 Q. We see that the totals from 2013 to 2017 cross that
 16 time. There may be nothing in this, but do you have any
 17 idea why the total number of requests peaked in 2015 and
 18 has fallen since?
 19 **A. I don't know, I'm sorry.**
 20 Q. So this is dated from 2013 to 2017. Can we look at the
 21 transparency report covering the first half of 2018.
 22 It's at tab B1 of your bundle.
 23 **A. Thank you.**
 24 Q. Please could we have APL000014 on the screen.
 25 Could we start with the first page, please. Thank

Page 50

1 Q. -- the table we can see it says:
 2 "Account-based requests generally seek details of
 3 customers' iTunes or iCloud accounts, such as name and
 4 address; and in certain instances customers' iCloud
 5 content, such as stored photos, email, iOS device
 6 backups, contacts or calendars."
 7 **A. I appreciate that, thank you.**
 8 Q. We see that there are a number of columns at the top,
 9 number of account requests received, number of accounts
 10 specified in those requests, number of account requests
 11 that were challenged or rejected, account requests where
 12 only non-content data was provided, content data
 13 provided, and then there's a percentage figure at the
 14 end.
 15 Could we have the row for the UK, please, with those
 16 columns on top retained. Thank you.
 17 So we see that the figure for the UK -- this is the
 18 first half of 2018 -- there were 263 account requests
 19 received. Then two columns along we have a figure of 28
 20 account requests which were challenged in part or
 21 rejected in full.
 22 Can you help us, in general terms why would account
 23 requests be challenged or rejected?
 24 **A. My understanding is that an account request would be**
 25 **challenged or rejected if a service wasn't proper, or if**

Page 52

<p>1 the request contained an inaccurate identifier.</p> <p>2 Q. It may be helpful if you look briefly at 8.2 of your</p> <p>3 statement; if we can keep that on the screen, please.</p> <p>4 So you give four categories there of the bases on</p> <p>5 which a request from a law enforcement agency will be</p> <p>6 rejected. So the first one is that the request has no</p> <p>7 valid basis or legal insufficiency --</p> <p>8 A. I'm sorry, which section are you looking at?</p> <p>9 Q. Sorry, 8.20.</p> <p>10 A. Yes.</p> <p>11 Q. Can you help us, who makes the assessment within Apple</p> <p>12 that the request has no valid legal basis?</p> <p>13 A. Our law enforcement and privacy team.</p> <p>14 Q. What is the meaning of the term "legal insufficiency"?</p> <p>15 A. So I would imagine where the request does not meet legal</p> <p>16 standard, but again I don't know, I'm not responsible</p> <p>17 for this area of our productions.</p> <p>18 Q. Understood.</p> <p>19 That second category you discuss in your statement</p> <p>20 is where the request is overly broad and does not set</p> <p>21 out specific time frames or users that the agency is</p> <p>22 seeking data for.</p> <p>23 A. Mm-hm.</p> <p>24 Q. Again, it's the Apple team that assesses whether the</p> <p>25 request is overly broad; is that correct?</p> <p style="text-align: center;">Page 53</p>	<p>1 A. Correct.</p> <p>2 Q. Can you help with -- and this may be outside, again,</p> <p>3 your expertise -- can you help with the standard that</p> <p>4 the Apple team applies in determining whether a request</p> <p>5 is overly broad?</p> <p>6 A. I don't know.</p> <p>7 Q. The third category in your 8.20 is that Apple doesn't</p> <p>8 hold any responsive data. That speaks for itself.</p> <p>9 The fourth is that the details provided by the law</p> <p>10 enforcement agency do not relate to an Apple account or</p> <p>11 device. Again, speaks for itself.</p> <p>12 Can we go back to the table. So we see that 28</p> <p>13 account requests from the UK were challenged in part or</p> <p>14 rejected in full. I suspect the answer is no, but do</p> <p>15 you have any idea why those requests were challenged?</p> <p>16 A. No.</p> <p>17 Q. Going back to the table, we see that 206 account</p> <p>18 requests were met with the provision of only non-content</p> <p>19 data, and there were no requests, if you go to the next</p> <p>20 column, where content data was provided.</p> <p>21 First of all, what is non-content data?</p> <p>22 A. So non-content data would be IP addresses, registration</p> <p>23 details, customer information, things along those lines.</p> <p>24 Q. Any idea why Apple would have provided only non-content</p> <p>25 data in response to those requests?</p> <p style="text-align: center;">Page 54</p>
<p>1 A. I don't have specific knowledge about these 206 cases,</p> <p>2 but I would imagine that at least some portion of those</p> <p>3 requests were only for non-content data. Again, as</p> <p>4 I mentioned earlier, requests for content generally go</p> <p>5 through our MLAT process, and so we wouldn't see</p> <p>6 requests coming from the UK, they would appear as if</p> <p>7 they were coming from the US.</p> <p>8 Q. So is it the case that those 263 account requests that</p> <p>9 are attributed to the UK, those would have come through</p> <p>10 the MLAT process?</p> <p>11 A. No, I'm sorry, what I'm saying is that any request that</p> <p>12 came through the MLAT process we likely would not have</p> <p>13 known that they came from the UK and so they likely</p> <p>14 would've been attributed to the US.</p> <p>15 Q. Understood.</p> <p>16 So what's the source of those 263 account requests</p> <p>17 that are received? How would they have come to Apple?</p> <p>18 A. Those would have come directly from the UK, is my</p> <p>19 understanding.</p> <p>20 Q. So in what circumstances would the UK send a direct</p> <p>21 request to Apple as opposed to going through the MLAT</p> <p>22 process?</p> <p>23 A. Again, I'm not certain, I don't believe that this table</p> <p>24 takes into account non-emergency -- I'm sorry, I don't</p> <p>25 believe that this table takes into account emergency</p> <p style="text-align: center;">Page 55</p>	<p>1 requests, so my assumption -- but this is an assumption</p> <p>2 and I can go back and check -- is that there are some</p> <p>3 requests for non-content data that are submitted</p> <p>4 directly to Apple.</p> <p>5 Q. We can see in the third row from the bottom of the</p> <p>6 table, if we could go to that, please, on the screen,</p> <p>7 the totals for the US. Thank you.</p> <p>8 So we have 2397 account requests received. 158 were</p> <p>9 challenged in part or rejected. Then we have a figure</p> <p>10 of 1239 requests for which non-content data was</p> <p>11 provided. Then 849 requests where content data was</p> <p>12 provided.</p> <p>13 You'll remember that the figure for the UK was zero.</p> <p>14 Any idea why the difference there between the</p> <p>15 provision of content data in response to US requests but</p> <p>16 not for the UK?</p> <p>17 A. Again, the number from the US are likely, and I do</p> <p>18 believe reflects, requests from other countries that</p> <p>19 came through MLAT. So it's a bit of a misleading</p> <p>20 statistic, although it says "United States", we</p> <p>21 generally don't have visibility into the underlying</p> <p>22 requesting nation when that nation goes through the MLAT</p> <p>23 process. So we categorise them as "United States", but</p> <p>24 they very likely may have come from a foreign</p> <p>25 government.</p> <p style="text-align: center;">Page 56</p>

<p>1 Q. Can we look at the very top of the table, so the row for 2 China. This may help us to test some of our 3 discussions. 4 So we see that there were 33 account requests 5 received from China. Zero were challenged in part or 6 rejected in full. There were 32 account requests for 7 which non-content data was provided. Then we have 8 a figure at the right-most column of 97 per cent. 9 You'll see from the table in front of you that the 10 relevant figure for the UK was 78 per cent. 11 Any idea why there's quite a large discrepancy 12 between the response rate for requests, for example from 13 China or other countries? The figure from the US is 14 87 per cent, if that's helpful. 15 A. I don't know specifically. What I can see is that 16 similarly there were zero account requests where content 17 data was provided here. So I don't know -- the answer 18 is I don't know. 19 Q. Can we go to page 11, please, of the transparency 20 report. Can we zoom in to the narrative at the top of 21 the table, please. Thank you. 22 So this is a table of worldwide government emergency 23 requests. In summary, the narrative at the top of the 24 table discusses the meaning of emergency requests and 25 how Apple responds to them.</p> <p style="text-align: center;">Page 57</p>	<p>1 We see -- if we can scroll down, please, for the 2 UK's row -- we see that 172 emergency requests were 3 received, 40 of them resulted in the provision of no 4 data, giving us a figure of 77 per cent in the 5 right-most column. Can we scroll down just to near the 6 bottom, to the US row, please. We have the figure of 7 89 per cent for the US. I appreciate from your answers 8 before this may not be something you will be able to 9 help us with, but any idea what may account for the 10 difference? 11 A. I don't, and I also don't know why the most requests are 12 coming from the UK. I don't know. 13 Q. I understand that Apple has provided some training to UK 14 law enforcement in terms of making requests from Apple. 15 Can you explain that briefly, please? If it helps, I'm 16 looking at 8.22 and 8.23 of your statement. 17 A. Absolutely. So, as I mentioned earlier, in response to 18 the CSIS study, that demonstrated that law enforcement's 19 biggest challenge in investigating cases isn't encrypted 20 data but it's a lack of understanding and knowledge 21 about how to get data that is relevant to their 22 investigations, we launched a worldwide training 23 programme and we targeted law enforcement agencies that 24 work on child sexual exploitation and other 25 child-related crimes to receive that training first.</p> <p style="text-align: center;">Page 58</p>
<p>1 We have given this training at a number of different 2 law enforcement-focused conferences where there's 3 an international law enforcement presence. We've also 4 trained members of the UK law enforcement, and we 5 conducted a training last March, we conducted a training 6 this past March and we're actually conducting a training 7 in July for the Metropolitan Police. 8 This training covers two basic topics. One is the 9 data that Apple maintains and how to obtain it, 10 including the type of process that we accept, and how, 11 just logistically, to go about requesting the data. The 12 second is more geared towards forensic experts in the 13 Apple ecosystem and what data may be maintained on 14 devices and how to look for different types of devices 15 that might maintain data that would otherwise be stored 16 on an encrypted device. 17 Q. Can you turn to tab B2 of your bundle, please, and could 18 we have NCA000354 on the screen, pages 4 and 5. 19 So this is an extract from evidence given on behalf 20 of the National Crime Agency to the UK Parliament's Home 21 Affairs Select Committee in April 2018. 22 We see, halfway down the first page, there's an 23 assertion there that there needs to be a significantly 24 enhanced role for industry, and then there is 25 a description of three simple achievable measures that</p> <p style="text-align: center;">Page 59</p>	<p>1 can be undertaken which will make a significant 2 difference in preventing image offences from occurring 3 in the first place. 4 Then we have three -- if we can call them "asks" of 5 the NCA as to what industry players should be doing. 6 Can I take you through those three asks and ask for 7 Apple's response to them. 8 So the first is the prescreening or the prefiltering 9 of material that is uploaded and downloaded. 10 Can I ask you what Apple's response to that ask is? 11 A. Yes. 12 So with respect to the filtering of known images, 13 I'm familiar with the technology, and it's effective. 14 With respect to technology that is being developed 15 to identify first-generation images, using things like 16 machine learning, my understanding is that that 17 technology is far less mature. From my own experience 18 reviewing images of child pornography, it is sometimes 19 very difficult to determine whether or not it truly is 20 child pornography; sometimes it's very clear. The way 21 that machine learning works -- again, I'm not 22 an engineer, but my understanding is that you 23 essentially train a computer to know what you know. And 24 so, as I'm sure you can imagine -- and my anticipation 25 is that for a technology that is far less mature, that</p> <p style="text-align: center;">Page 60</p>

<p>1 relies on subjectivity, I imagine, you know, that we 2 could anticipate that there would be a large number of 3 false positives that could result from that technology. 4 And so, use of that sort of technology outside of 5 social media, particularly on private channels where 6 a user has an expectation of privacy, it sort of raises 7 questions about its effectiveness and the implications 8 on user privacy. 9 Q. Can we turn to the second ask, please, which is at the 10 top of page 5, if we could zoom in on -- thank you very 11 much: 12 "Industry platforms that have the appropriate 13 safeguards in place could be granted a kitemark. In 14 particular, this could be piloted with those platforms 15 that are specifically targeted at children." 16 What is Apple's response to that ask? 17 A. Depending on how it's implemented, we believe that 18 kitemarking can be quite effective. We use kitemarking 19 on our App Store. We have a curated kids' category on 20 our App Store and, as I mentioned, all of our apps are 21 subject to a high level of scrutiny and restrictions 22 before they make it own to our App Store. Our kids' 23 category is far higher, and so, for apps that are 24 curated into our kids' category -- if you have children, 25 I highly recommend that you take a look -- the apps in</p> <p style="text-align: center;">Page 61</p>	<p>1 our kids' category prohibit, for example, freeform 2 communication. So you will not find any social media 3 apps on the kids' category. There are enhanced privacy 4 controls. Any in-app purchases are required to be 5 behind a parental gate, for example. 6 And we believe that these are protections that are 7 important for children, and so this form of kitemarking 8 we believe has been very effective. 9 Q. Can you just remind me again -- so there were two apps 10 that Apple removed from the App Store for a time. They 11 were Tumblr and Telegram. 12 A. There were more apps than two, but those are the two 13 I mentioned, yes. 14 Q. Understood. 15 I suppose the question that a member of the public 16 hearing that would have is, if Apple would be -- rowing 17 back, if we see from that experience that there were 18 apps that were left on the App Store for a time at 19 least, that evidently didn't have the appropriate 20 safeguards in place, is there a case for a more 21 intensive review process from Apple so that such 22 platforms are never -- are put on the App Store at all? 23 A. We're certainly open to suggestions about our app 24 developer programme and the restrictions that we have. 25 Again, we only -- we can only make determinations about</p> <p style="text-align: center;">Page 62</p>
<p>1 apps based on the information that we have, which is 2 often incomplete, based on the nature of the apps, and 3 so we do our very best to ensure that the apps that we 4 put up on our App Store meet our guidelines. 5 If law enforcement becomes aware that an app has not 6 met the requirements and is putting children at risk, we 7 encourage you to let us know and we will conduct a very 8 thorough investigation. 9 Q. There is, I think, a theme that's come through in your 10 evidence of Apple taking quite a reactive approach in 11 this space, so I think that's how you described the ICS 12 team as working, as being quite a reactive team, and 13 thus its relatively small headcount and small resources 14 that are available to it. 15 Is there a case for Apple taking a more proactive 16 role to make sure that its products and services aren't 17 used for this type of abuse? 18 A. If I've given the impression that Apple takes a reactive 19 role to child safety, then I have done us a grave 20 disservice. 21 When I talk about my team, my team conducts 22 investigations, and so -- in terms of the investigations 23 side of the house. And so, to that extent, we can be 24 reactive. From the child safety perspective, we work 25 with business groups to draft policies, to ensure that</p> <p style="text-align: center;">Page 63</p>	<p>1 our platforms are meeting their responsibilities, to 2 ensure that we're following the law and that we're 3 following our morals and doing the right thing. 4 Apple is incredibly proactive when it comes to child 5 safety. As I mentioned, we take great care in ensuring 6 that everyone who uses our platform is safe and secure. 7 And part of the way that we do that is through the 8 features that are built into both of our -- both our 9 hardware and our software and the programmes that we 10 implement surrounding our supply chain. 11 So I don't think it's a fair characterisation that 12 we are a reactive company, perhaps some of the things 13 that you have seen social media companies doing to 14 moderate their content may be driving that assertion. 15 Q. Can I ask for your response to the third ask, which is 16 certain industry members ring-fence a portion of their 17 R&D budgets to develop and design safeguards into all 18 their products. 19 So, first of all, is this something that Apple 20 already does? 21 A. So -- so in terms of ring-fencing budgets, we certainly 22 believe that it is imperative to dedicate resources to 23 child safety. 24 As I mentioned earlier, we do not -- that's not 25 a model that we use in terms of ring-fencing, we believe</p> <p style="text-align: center;">Page 64</p>

<p>1 that we determine what is necessary, what is appropriate 2 and what is important to implement, and we throw as many 3 resources as necessary at those projects and programmes, 4 and those resources can be spent throughout the company 5 from multiple business groups, and we do not spend 6 resources tallying the resources that we spend to keep 7 people safe.</p> <p>8 Q. On resources, can you tell us if Apple makes any 9 contribution to NGOs that are working in this field of 10 online-facilitated child sexual abuse?</p> <p>11 A. So, first of all, Apple takes a very employee-driven 12 approach to donations. Apple will match employee 13 donations up to \$10,000 per year, and so a large 14 proportion of Apple's giving is through that programme, 15 and I do not know what portion of those donations relate 16 to child safety.</p> <p>17 With respect to the broader question of Apple's 18 corporate giving to child safety, again, we take a very 19 holistic approach, given the nature of our ecosystem, 20 given the ways in which our products impact the world 21 and the fact that it's not limited to online.</p> <p>22 So, again, we do have significant programmes in 23 place around the world related to our supply chain in 24 terms of ensuring that there is no child labour in our 25 manufacturing, and ensuring that there are resources in</p> <p style="text-align: center;">Page 65</p>	<p>1 place, for example, when child labour is found, that 2 that child gets returned to their family, that education 3 is paid for, and that there is a job waiting for that 4 child at the factory once the child turns of age. We 5 also -- I'm sorry?</p> <p>6 Q. Sorry, no, please carry on.</p> <p>7 A. We also have initiatives around -- we recently announced 8 a news literacy project. One of the harms that was 9 identified in the Online Harms White Paper, for example, 10 was the proliferation of inaccurate information and, as 11 a news service provider, that's something that we care 12 about, and so we launched a partnership with several 13 NGOs to provide education and information to children, 14 educators and parents around news literacy, being 15 an informed consumer of news and being able to better 16 judge accurate versus inaccurate information in the 17 news.</p> <p>18 Specific to online child safety, I believe in my 19 report I reference some donations that we've made -- 20 could you reference the paragraph?</p> <p>21 Q. 9.2.</p> <p>22 A. And so -- so we have made specific donations to NGOs and 23 non-profits that are working very specifically in the 24 space of online child safety. Those donations, as with 25 all of Apple's donations, tend to be targeted at</p> <p style="text-align: center;">Page 66</p>
<p>1 specific opportunities rather than blanketing NGOs with 2 funding.</p> <p>3 And so, for example, in the last year we spent 4 \$250,000 specific to online child safety and that 5 reflects donations that we've made to, for example, 6 Thorn, which is an organisation in the United States 7 that is looking and was developing technology 8 surrounding facial recognition technology, which is 9 something that we -- we value, and they were using 10 facial recognition technology to attempt to identify 11 victims of sexual trafficking and sexual abuse on the 12 dark web. So when we learned of that opportunity -- 13 again, a very targeted opportunity -- we provided them 14 with the funding to do that.</p> <p>15 We worked with an organisation that created a tool 16 for a law enforcement in North America to identify 17 paedophiles using peer-to-peer networks to trade child 18 pornography, and they -- we actually had a meeting with 19 them along with some of our technologists and engineers 20 to better understand our tool and see how we could 21 provide assistance.</p> <p>22 This number does not reflect man-hours and that 23 meeting on this -- this is strictly dollars that were 24 provided.</p> <p>25 But -- but upon meeting with that organisation and</p> <p style="text-align: center;">Page 67</p>	<p>1 understanding the tool that they had built, we realised 2 that there were certain tools that they weren't taking 3 advantage of that we felt could greatly enhance their 4 ability to identify paedophiles, particularly those 5 using VPNs, and so we paid for that technology.</p> <p>6 Q. Can we, on the same subject of asks, turn to the 7 government's Online Harm White Paper.</p> <p>8 The inquiry understands that the consultation 9 process is ongoing, so you may be limited in what you 10 are able to say at this stage, but insofar as you are 11 able to, could you please provide Apple's views on the 12 proposals in the White Paper, specifically that there 13 should be a regulatory framework rather than relying on 14 self-regulation and, secondly, that there should be 15 codes of practice issued by an independent regulator in 16 the UK.</p> <p>17 A. So as you mention, the White Paper -- we have not fully 18 processed the White Paper, we are still in discussions, 19 but what I can say is that we do very much appreciate 20 the differentiation the White Paper made between 21 one-on-one communications and social media 22 communications. We, too, value that distinction and 23 believe that private communications should be treated 24 differently than communications through a social media 25 platform.</p> <p style="text-align: center;">Page 68</p>

<p>1 We also appreciate that the White Paper called out 2 the importance of parental controls and empowering 3 parents to take better control over their child's 4 devices.</p> <p>5 We also appreciate the Online Harms White Paper 6 mentioned this information as a potential harm for 7 children online, which we identify as well.</p> <p>8 In terms of -- in terms of regulating technology, we 9 are generally in favour of additional regulation, but 10 I think it depends on what that looks like, and the 11 devil really is in the details, so we're happy to have 12 additional conversations about what that detail looks 13 like. It's hard to comment in the abstract.</p> <p>14 Q. Can I ask you a question on one point that I raised 15 there? I appreciate, again, you may not be able to 16 answer at this stage. You said that you valued the 17 distinction made between private communications and 18 social media platforms.</p> <p>19 Given what we discussed earlier about the potential 20 of leakage from a social media platform to private 21 communication, where conversations are taken from social 22 media to a means such as iMessage, and so forth, does 23 Apple have any position about the extent to which 24 private communications should be regulated?</p> <p>25 A. I can't speak specifically to regulation, but our</p> <p style="text-align: center;">Page 69</p>	<p>1 position is that private communications are private, 2 and, as such, we have encrypted them, that the benefit 3 to society and the benefit to our customers is in 4 ensuring secure and private communications.</p> <p>5 Q. One last question from me.</p> <p>6 The inquiry heard evidence from a mother of a victim 7 of online-facilitated child sexual abuse, and her 8 suggestion was that industry should pay a compensation 9 where industry has failed in its duty of care towards 10 the child. Does Apple have any position on that?</p> <p>11 A. I don't.</p> <p>12 MR KRISHNAN: Those are my questions. Thank you very much 13 for the session. Can you wait there in case the chair 14 and panel have any questions?</p> <p>15 THE CHAIR: No, thank you, we don't have any questions. 16 Thank you very much, Ms Polinsky.</p> <p>17 A. I did have one area of clarification, if that's okay.</p> <p>18 MR KRISHNAN: Yes, of course.</p> <p>19 A. So you had asked me about age restrictions on iMessage 20 and FaceTime, and I wanted to just clarify that our 21 parental controls are designed for children up to 13, 22 and that parents, we encourage parents to use those 23 parental controls and they can be used to control the 24 use of iMessage and FaceTime.</p> <p>25 And I understand that -- I also just would like to</p> <p style="text-align: center;">Page 70</p>
<p>1 point out that in terms of the use of iMessage and 2 FaceTime, unlike other platforms, our software is very 3 much integrated with our hardware, and so, when you're 4 talking about the use of these apps, you're talking 5 about the use of our devices, which tend to be quite 6 expensive, and so, although it's certainly possible for 7 children to buy our devices -- no one stops a child from 8 coming into our store -- I would imagine that parental 9 controls are a very powerful tool for parents who are 10 providing devices for their children.</p> <p>11 MR KRISHNAN: Thank you very much. Chair, is that 12 an appropriate point to break for lunch. And perhaps 13 come back a little bit earlier for the afternoon 14 session?</p> <p>15 THE CHAIR: Yes. We'll return at 1.45.</p> <p>16 MR KRISHNAN: Thank you, chair. 17 (12.35 pm) 18 (The short adjournment) 19 (1.45 pm) 20 (The court went into closed session) 21 (2.55 pm) 22 (In Open Session)</p> <p>23 MS CAREY: Thank you, chair, we're turning now to the 24 evidence of Mr Milward from Microsoft and can I ask that 25 he is sworn?</p> <p style="text-align: center;">Page 71</p>	<p>1 MR HUGH CHARLES MILWARD (affirmed)</p> <p>2 Examination by MS CAREY</p> <p>3 MS CAREY: Would you state your full name for the inquiry, 4 please?</p> <p>5 A. Yes, my name is Hugh Charles Milward.</p> <p>6 Q. Mr Milward, a little about you, firstly. I think you 7 are the senior director for corporate, legal and 8 external affairs at Microsoft UK?</p> <p>9 A. That's correct.</p> <p>10 Q. In a nutshell, what is it, in layman's terms, that you 11 actually do?</p> <p>12 A. So I sit on the UK leadership team and I run the part of 13 the business that looks after our corporate affairs, 14 our -- all our legal work, that's the closure of our 15 deals with our customers and our external relations 16 work.</p> <p>17 That means that I'm the most senior person in the UK 18 in the bit of the business that looks specifically at 19 these kinds of issues.</p> <p>20 Q. I think you say in your statement, at paragraph 4, that 21 you oversee a range of corporate functions in the UK, 22 and that you sit on both the UK and the European 23 leadership teams.</p> <p>24 How long have you been working for Microsoft?</p> <p>25 A. I joined Microsoft in 2012.</p> <p style="text-align: center;">Page 72</p>

1 Q. Prior to that, did you have any professional experience
 2 dealing with CSEA-type concerns?
 3 **A. To a small degree, I had a similar function working for**
 4 **Starbucks, and I worked with John Carr, one of the great**
 5 **campaigners for -- for children's rights, to try to**
 6 **remove the ability to access adult content in Starbucks**
 7 **stores across the country.**
 8 Q. In fact, we're going to be hearing from Mr Carr next
 9 week, and one of the things he attests to is the Wi-Fi
 10 arrangements at Starbucks, which at one stage enabled
 11 CSA to be downloaded in their stores. I'll let him deal
 12 with that evidence, if I may.
 13 Just concentrating on Microsoft, would you be able
 14 to tell us, please, a little bit about Microsoft? I'm
 15 aware from your statement that Microsoft UK was
 16 established in 1997. You have, I think, 5,000 employees
 17 in the UK. Headquarters is based in Reading, and
 18 I assume Microsoft UK is a subsidiary of Microsoft Inc?
 19 **A. Yes, Microsoft UK is a subsidiary, but I am actually**
 20 **speaking -- while I am an employee of Microsoft UK, I'm**
 21 **actually speaking for the whole of the corporation.**
 22 Q. So we can have a little bit of perspective on how the UK
 23 sits with Microsoft globally, do you have any idea of
 24 the number of employees worldwide?
 25 **A. There are around 110,000 employees worldwide. The UK**

Page 73

1 Q. Before we come to the various teams, I'd like your
 2 evidence, please, on the types of different products and
 3 services that Microsoft offers, and then, if we can look
 4 at what form of child sexual abuse harm is perhaps most
 5 commonly encountered on those different products.
 6 Can we look, please, at the products firstly.
 7 I think the products include Office 365 and
 8 Dynamics 365. Just in a nutshell, what are those two
 9 products?
 10 **A. Office 365 is a suite of products which typically**
 11 **include Word, Excel, PowerPoint, and so forth. The 365**
 12 **element means that it's in the cloud, and I can explain**
 13 **what that means, if it's required.**
 14 Q. Well, can I pause you there to say that I assume, based
 15 on what you told us about Office 365, that that is not
 16 really one of the products that Microsoft offers where
 17 you encounter CSAM material?
 18 **A. Well, actually, we do, and that is because OneDrive,**
 19 **which is a cloud storage solution, forms part of**
 20 **Office 365 and, equally, it includes Outlook, which is**
 21 **an email service, and we occasionally see elements of**
 22 **CSEAI appearing in email.**
 23 Q. Effectively, email being used to share that imagery?
 24 **A. Correct.**
 25 Q. Right. Dynamics 365, though, you were going on to say

Page 75

1 **has under -- just under 5,000 of them.**
 2 Q. Microsoft UK, I think, you, in your senior director
 3 role, have a reporting responsibility, do you not, to
 4 the global chief online safety officer?
 5 **A. Yes, so Jacqueline Beauchere is our global online safety**
 6 **officer. She sits in the same organisation as I do. We**
 7 **both report to -- ultimately, to Brad Smith, who is our**
 8 **president. So I don't report into her, but we both**
 9 **report into the same group.**
 10 Q. And if Microsoft Inc want to disseminate either some
 11 learning or a new policy that's CSEA-related, who is it
 12 who is responsible for implementation of that in the UK?
 13 Is that you?
 14 **A. So as far as engineering is concerned, there are parts**
 15 **of our engineering teams that sit all over the world.**
 16 **Some of those are in the UK. So the implementation of**
 17 **a new policy that governs, for example, Bing search,**
 18 **some of that will be done directly from the Bing**
 19 **engineering team in Redmond, in the US, integrating it**
 20 **into the UK. There are several other functions that**
 21 **will be my responsibility, but it is -- it's very**
 22 **disaggregated, not least because we do, in some of our**
 23 **work -- our "follow the sun" mechanism, so that you have**
 24 **people who are on point for various aspects all over the**
 25 **world.**

Page 74

1 you could expand upon. Please do.
 2 **A. We should think about that as -- as CRM, customer or**
 3 **client relationship management software. Effectively,**
 4 **it's a sort of database-type software. We don't see**
 5 **that as being in scope here.**
 6 Q. We'll put that to one side then.
 7 You mentioned hardware such as Surface devices and
 8 Xbox. What are Surface devices?
 9 **A. Surface is a computer much like this, it's a suite of**
 10 **different computers of different sizes that do slightly**
 11 **different things, so it's hardware and we compete with**
 12 **other computer manufacturers such as HP or Dell and**
 13 **others.**
 14 **Xbox is a gaming platform, and we compete with --**
 15 **typically with PlayStation.**
 16 Q. Yes.
 17 **A. There are a number of other services that I think**
 18 **probably are in scope that relate to Xbox, including**
 19 **Mixer, which is a platform for sharing video content, so**
 20 **typically, gamers will record their game play and then**
 21 **share it with other gamers. It's actually an extremely**
 22 **popular pastime for younger people.**
 23 **Equally, there are a number of platforms that we own**
 24 **including Skype, LinkedIn, GitHub, which is a sharing**
 25 **platform for open-source coding, and one or two others**

Page 76

1 **that really fall out of the scope for, I mention, your**
 2 **inquiry.**
 3 Q. If we can focus then on your evidence on those platforms
 4 or products that most commonly are used for the abuse of
 5 children and the proliferation of that kind of imagery.
 6 Help us with Xbox and Mixer. Xbox Live, I think is
 7 often used for grooming of young children, and do I take
 8 it, from what you've said, that if they are able to
 9 share video content, is that something you could also
 10 share illegal imagery through Mixer --
 11 **A. Yes, it --**
 12 Q. -- or not so much if you're videoing the gaming?
 13 **A. It is possible to share video content of the gamer**
 14 **playing the game, for example, and that gamer playing**
 15 **the game could be doing pretty much anything. So, yes,**
 16 **that is possible.**
 17 Xbox Live is a -- it's a partly open and partly
 18 closed network that allows players to share information
 19 while they're playing a game on Xbox.
 20 Mixer is -- is effectively an open platform that
 21 allows people to post video play of -- of themselves,
 22 either live video play, as it's taking -- as the game is
 23 being played, or files of play that's already happened.
 24 Q. Right.
 25 Is it also right that Microsoft has a search engine

Page 77

1 important to remember they may not be on all products,
 2 but certain products facilitate potentially the
 3 perpetrators who are intent on that kind of criminality.
 4 I'd like to just deal with the structure, please, of
 5 Microsoft and the number of teams that are involved in
 6 keeping children safe online and, in particular, trying
 7 to combat the problem of child sex abuse material.
 8 Can we start, please, at paragraph 11 in your
 9 statement, Mr Milward. I think you say this, that there
 10 is a large number of teams and individuals across
 11 Microsoft whose work focuses on, and otherwise impacts
 12 on, online safety. You say:
 13 "It is impossible to provide a precise figure. We
 14 estimate it to be in the thousands."
 15 Are you talking about globally?
 16 **A. Globally.**
 17 Q. First team is the legal team, who work globally on your
 18 standards, statutory reporting to NCMEC that the chair
 19 and panel have already heard about, and they are lawyers
 20 based in multiple countries; is that right?
 21 **A. That's correct.**
 22 Q. You say at the first bullet point that there is
 23 a centralised team such as Microsoft Digital Crimes
 24 Unit, just helps please with what the DCU, Digital
 25 Crimes Unit, is?

Page 79

1 called Bing?
 2 **A. That is correct.**
 3 Q. What type of harm is most commonly encountered on Bing,
 4 presumably searching for indecent imagery?
 5 **A. That is correct, yes. So Bing is typically search**
 6 **queries that are used to find, discover, information**
 7 **that's out there on the internet. Some of that**
 8 **information out there can be CSEAI content and,**
 9 **therefore, Bing can surface that content.**
 10 Q. So in giving your evidence, one needs to have in mind
 11 the use of Bing as the search engine, perhaps for
 12 looking for the content, sharing it, would that
 13 potentially be through OneDrive?
 14 **A. So content can be shared through OneDrive, typically**
 15 **images and videos.**
 16 **Grooming can take place on -- on Xbox.**
 17 **Searching for imagery can take place on Bing --**
 18 Q. Yes.
 19 **A. -- and there's a certain amount of grooming that can**
 20 **take place in the games that are used on Xbox.**
 21 Q. If one thinks about live streaming, is that something
 22 that could take place via Skype?
 23 **A. Indeed, Skype is also very much in scope.**
 24 Q. I start with that because we will look at the different
 25 types of harm as we go through your evidence, but it's

Page 78

1 **A. So the Digital Crimes Unit is a collection of engineers,**
 2 **analysts and lawyers, whose sole purpose is to try to**
 3 **clean up the internet of various types of harm, and so**
 4 **they spend a lot of time investigating and taking down**
 5 **large botnets. They are typically --**
 6 Q. Can you help with the "botnet"?
 7 **A. A botnet is a -- it's a network of -- think about it as**
 8 **a network of viruses that all report into a --**
 9 **a controller. And that controller is typically either**
 10 **a nation state government or an actor on behalf of**
 11 **a nation state government or it will be a criminal**
 12 **organisation of some kind.**
 13 **So we do a lot of work on -- on these kind of cyber**
 14 **attacks and -- and networks.**
 15 **Equally, that team does a lot of work around child**
 16 **sexual abuse.**
 17 Q. I think the Digital Crimes Unit is responsible in part
 18 for the development of PhotoDNA, and we're going to come
 19 on to deal with PhotoDNA as a separate topic.
 20 Let me just finish with the teams, so that everyone
 21 is clear about the structure.
 22 There are content moderators that monitor
 23 Microsoft's products. Can you give us an indication of
 24 how many moderators there are employed by Microsoft?
 25 **A. I can't say precisely how many there are, but what I can**

Page 80

<p>1 say is that the job -- that the number of moderators is</p> <p>2 roughly reflective of the number of incidents that we</p> <p>3 see on our platforms and services. And so, you know,</p> <p>4 typically, we will make around 5,800 referrals to NCMEC</p> <p>5 a year. The content moderation team is geared to be</p> <p>6 able to respond to that many and that is -- that's --</p> <p>7 that is the number that they -- that they see, not</p> <p>8 because they're not working hard enough or because there</p> <p>9 aren't enough of them, it's that those are the number of</p> <p>10 referrals that we see coming through our platforms.</p> <p>11 So the team we have in place there is a double team,</p> <p>12 so that any referral or any image that needs to be</p> <p>13 assessed is sent to both teams at the same time to be</p> <p>14 dual analysed.</p> <p>15 So there is a certain amount of replication that</p> <p>16 takes place across the content that -- that content</p> <p>17 review process.</p> <p>18 Q. And why is it that Microsoft dual analyses a suspected</p> <p>19 indecent image?</p> <p>20 A. So if we see an image that is, for example, shared from</p> <p>21 someone's OneDrive, with another user, and it is flagged</p> <p>22 in -- through a number of mechanisms as being</p> <p>23 potentially a child sexual abuse image, it goes through</p> <p>24 these two twin tracks of review at the same time, and</p> <p>25 those twin tracks really need to align and both agree</p> <p style="text-align: center;">Page 81</p>	<p>1 that the content is, in fact, child sexual abuse.</p> <p>2 We assess those against a matrix of -- of abuse</p> <p>3 that's commonly used across the industry. I can go into</p> <p>4 that matrix, if it's required. It's pretty harrowing.</p> <p>5 Q. I'm not sure it's going to be necessary to descend into</p> <p>6 that detail, but is the purpose of the dual analysis to</p> <p>7 ensure that the reports that go to NCMEC are accurate?</p> <p>8 A. They are to do -- to ensure that they're accurate, so to</p> <p>9 give us a very firm basis, and a firm basis for law</p> <p>10 enforcement to be able to take action.</p> <p>11 It's also because, if we conclude that it does</p> <p>12 contain child sexual abuse material, then we will close</p> <p>13 the user's account, and bearing in mind that on, you</p> <p>14 know, some platforms, that might just restrict access to</p> <p>15 that service, on Microsoft, if we close their account,</p> <p>16 it removes access to absolutely everything to do with</p> <p>17 Microsoft.</p> <p>18 So, for example, if they are sharing an image and</p> <p>19 it's found on Xbox, then they will lose access to all of</p> <p>20 their storage on OneDrive, lose access to all their</p> <p>21 e-mails on Outlook. It's a very severe punishment and</p> <p>22 we want to be sure that we've got it right at the point</p> <p>23 at which we do that.</p> <p>24 Q. Is there any circumstance in which you would find</p> <p>25 a child sexual abuse image and that punishment is not</p> <p style="text-align: center;">Page 82</p>
<p>1 imposed?</p> <p>2 A. There are no circumstances that I'm aware of.</p> <p>3 Q. It's not the case that if someone's made a mistake or</p> <p>4 come by it by error or anything like that, there's</p> <p>5 a mechanism by which you can impose a different sanction</p> <p>6 or take a different punishment, for want of a better</p> <p>7 phrase?</p> <p>8 A. Well, that's why we want to ensure that there is this</p> <p>9 level of certainty, and so the image is scanned by</p> <p>10 two -- it's reviewed by two teams, and then it's</p> <p>11 reviewed by a third to provide that absolute conclusion</p> <p>12 at the end of that dual process.</p> <p>13 Q. Is there any appeal process in the event that you shut</p> <p>14 down someone's access to their Microsoft products?</p> <p>15 A. There is not currently an appeals process. But the --</p> <p>16 a user who has had their account taken away can resort</p> <p>17 to court, if they wish. We've not yet had that.</p> <p>18 Q. Finally on content moderators, are they based in the UK,</p> <p>19 US?</p> <p>20 A. The content moderators are based in the US.</p> <p>21 Q. Is there any difficulty in aligning what is illegal in</p> <p>22 the United States of America with potentially UK laws?</p> <p>23 A. Well, again, we review that content against this -- it's</p> <p>24 roughly a 4x4 grid, and that is industry-wide practice,</p> <p>25 and so that would apply whichever nation it happens to</p> <p style="text-align: center;">Page 83</p>	<p>1 be in.</p> <p>2 Q. There's no danger of something being classified as an</p> <p>3 illegal image in the UK, but not in the States, or vice</p> <p>4 versa, and someone losing access to all of their</p> <p>5 Microsoft products or platforms?</p> <p>6 A. We would block, in the case of four of the 4x4 -- four</p> <p>7 of the squares of the 4x4 grid, if you put it that way.</p> <p>8 So you are looking at the most egregious and looking at</p> <p>9 children who are very definitely under age.</p> <p>10 Now, I know in some countries there are different</p> <p>11 age limits as to what is illegal, but, again, we will</p> <p>12 block the more egregious end and where there is</p> <p>13 absolutely no doubt that this is illegal content.</p> <p>14 Q. Can I just ask you this -- you said you were unable to</p> <p>15 provide the number of moderators. Can I just ask this:</p> <p>16 is that because you don't know the figure and it's not</p> <p>17 ascertainable or is it because Microsoft would rather</p> <p>18 keep that information private?</p> <p>19 A. Well, we would rather keep that information private. It</p> <p>20 is in the tens, not in the hundreds or in the thousands,</p> <p>21 and bear in mind that this is the team that reviews</p> <p>22 content to determine whether it is child sexual abuse</p> <p>23 material or not. This is not the limit to the resources</p> <p>24 that are placed on tackling this whole issue, which,</p> <p>25 again, is in the thousands.</p> <p style="text-align: center;">Page 84</p>

1 Q. Yes.
 2 In addition to moderators, I think you say you have
 3 engineers around the world dedicated to supporting
 4 a range of technologies, including PhotoDNA?
 5 **A. Yes, could I just clarify the word "moderators" there?**
 6 Q. Yes.
 7 **A. So I guess "moderators", we would typically use that**
 8 **phrase to refer to people who are involved or have**
 9 **access to a live conversation and are able to step in**
 10 **and effectively moderate the discussion as it takes**
 11 **place.**
 12 **And, you know, we can -- I imagine we'll go on to**
 13 **that, but there are some new technologies that are**
 14 **coming online that are helping us to do that better and**
 15 **better, but what we're talking about in terms of**
 16 **determining whether a piece of content is child sexual**
 17 **abuse material or not are not actually doing live**
 18 **moderation.**
 19 Q. So that we are clear, you have those that are
 20 potentially monitoring and stepping into a discussion if
 21 they deem it to be inappropriate or perhaps even
 22 illegal?
 23 **A. Yes.**
 24 Q. And you also have the analysts who effectively determine
 25 whether there is illegal content?

Page 85

1 a key role in this area. Are you able to assist with
 2 the budget for that unit?
 3 I'm looking at your paragraph 12, if that assists?
 4 **A. Yes, I can't assist with that. And that's largely**
 5 **because the unit does a lot of work in terms of**
 6 **maintaining the security of the internet and of our**
 7 **customers, and around -- of cyber security and other**
 8 **aspects. What we tend not to do is disaggregate the**
 9 **elements that deal particularly with child sexual abuse**
 10 **material.**
 11 **And the cyber security work, you know, can be -- all**
 12 **of it can go through peaks and troughs in activity and**
 13 **in focus, depending on whether we are currently**
 14 **suffering a global or a more narrow cyber security**
 15 **attack, so resources are deliberately designed to be**
 16 **flexible to be able to move in certain instances where**
 17 **they need to.**
 18 Q. I think you do say in your statement, though, that the
 19 precise resources of the Digital Crimes Unit has
 20 an annual budget of several millions of US dollars?
 21 **A. That's correct.**
 22 Q. I think you went on to say it's not possible to give
 23 a precise proportion of the time the Digital Crime Unit
 24 spends on child sexual abuse and exploitation, but it is
 25 one of the areas they cover?

Page 87

1 **A. That is correct.**
 2 Q. All right.
 3 We just dealt with engineers. I think there are
 4 also public policy and government affairs professionals
 5 who engage with the policymakers. Would it be people in
 6 those teams who would perhaps engage with UK Government
 7 in relation to the White Paper that's recently been
 8 published?
 9 **A. That's correct, and they would typically sit in my team.**
 10 Q. Obviously, customer services and support staff, and then
 11 researchers and engineers who examine new technical ways
 12 of tackling child sexual abuse material. Can you give
 13 us an idea of the scale of numbers that Microsoft employ
 14 in that team and those departments?
 15 **A. A good example of that is the Microsoft research**
 16 **facility in Cambridge. While the majority of its focus**
 17 **is on the development of AI and machine learning and**
 18 **various other aspects, there are parts of their learning**
 19 **of what they are developing around machine learning that**
 20 **can be applied to this sort of situation. And, you**
 21 **know, Cambridge employs around 170 PhD-level computer**
 22 **scientists, who are working predominantly on AI, but any**
 23 **spark of new innovation from that facility could be**
 24 **harnessed in the fight against child sexual abuse.**
 25 Q. In terms of the Digital Crimes Unit, clearly they play

Page 86

1 **A. That's correct.**
 2 Q. Can you help in any way to expand a little bit about the
 3 work the DCU does in relation to child sexual abuse?
 4 **A. To give an example of the difficulty in disaggregating**
 5 **that, if you've got a, you know, effectively a criminal**
 6 **mastermind that is running a network of infected**
 7 **machines across the world, one of the -- one of the**
 8 **mechanisms that they will use to try to earn money will**
 9 **be to involve themselves in various aspects of child**
 10 **sexual abuse and that sort of content. So you actually**
 11 **find that in some of these networks there is**
 12 **a bleed-over between the different types of -- of**
 13 **criminal activity that is taking place.**
 14 Q. Does it follow, from what you've said, that there is no
 15 specific child sexual abuse budget within Microsoft UK?
 16 **A. That is correct. The budget is held globally.**
 17 Q. Is there a specific budget set aside for maintaining and
 18 improving PhotoDNA?
 19 **A. The -- there isn't. And that's largely because it's**
 20 **a sort of "always on" project of what we could harness**
 21 **from other parts of the engineering work that's taking**
 22 **place in Microsoft that could be brought in to the**
 23 **development of technologies like PhotoDNA.**
 24 **And so we don't have a specific budget that says**
 25 **"This is just for the development of PhotoDNA", it's**

Page 88

<p>1 more about, how could any new engineering or AI 2 development be used to improve or -- or form part of the 3 next generation of PhotoDNA? 4 Q. Is there any budget that is set aside to support those 5 institutions that Microsoft is either a member of or 6 donates money to? 7 A. Yes, there is. And we -- there are a number of those 8 organisations that we fund. 9 I wouldn't say that there was a budget for it, 10 I would say that we just fund them. 11 Q. Right. 12 A. So you could say that the budget was the aggregate sum 13 of all the membership fees for those organisations. 14 Q. Yes, I ask that for this reason: I think you're aware, 15 Mr Milward, that one of the National Crime Agency's key 16 asks is that a portion of a budget -- I think they 17 suggested the research and design budget, but call it 18 what you will -- is set aside for combating this area of 19 harm. So I was just trying to understand how Microsoft 20 arranges itself financially to see what you might say to 21 that NCA ask of industry? 22 A. Yes, so our R&D budget is probably well in excess of 23 a billion dollars a year, and there is any amount of 24 that that will be about the development of new ideas and 25 new technologies that could be applied to this area.</p> <p style="text-align: center;">Page 89</p>	<p>1 Q. Do you think it is realistic for the National Crime 2 Agency to make such an ask of a company such as 3 Microsoft when there's a budget of a billion potentially 4 available? 5 A. I think, like any field, the work is never enough. And, 6 you know, in many respects, if we wanted to truly stamp 7 out all of this, then we would devote 100 per cent of 8 everything to doing so, and all other organisations 9 might do the same. I don't think that's a realistic 10 proposition. We choose not to have one-on-one policing, 11 for example. We choose to say that there is a -- you 12 know, kind of realistic element of -- of what we will 13 tolerate as a nation, as a society. 14 And I think, for Microsoft, we feel that the 15 development that we're making around PhotoDNA, the 16 investments we're making, are -- are good. There's 17 always more work to be done. 18 I do think it's worth a conversation with NCA 19 about -- about how much the budget is the constraining 20 factor and how much the constraining factors are 21 actually not budget-related. 22 Q. Is it you or your team that is responsible for liaising 23 with the National Crime Agency, for example, or the 24 NPCC? 25 A. It's not my team, but it's part of the same -- the same</p> <p style="text-align: center;">Page 90</p>
<p>1 part of the -- it's part of the organisation that I -- 2 I represent. 3 Q. The chair and panel may be interested to know a little 4 bit more about how effective a liaison interaction there 5 is between Microsoft and law enforcement. 6 Can you help with the number of meetings that are 7 attended or the forums that are gone to where this kind 8 of topic is discussed? 9 A. So we think we have a very good relationship with law 10 enforcement of different kinds, including the NCA. 11 Inevitably, there will be -- we can improve, and, you 12 know, I would love to have the -- to keep the 13 conversation going about how we could improve that. But 14 we -- we -- we're very -- we're very focused on what it 15 is that we can do that will improve the relations not 16 just within the industry, but with law enforcement and 17 within those NGOs who are dedicated to tackling this. 18 I mean, a good example of that is the Hackathon -- 19 and for "Hackathon", I think read "significant 20 brainstorming resulting in an engineering solution", 21 that's really what we mean by "Hackathon" -- but that 22 took place in November of last year, where we brought 23 together a range of engineering teams, a range of 24 technology companies. The Home Secretary attended as 25 well, and the result of that, of getting the right</p> <p style="text-align: center;">Page 91</p>	<p>1 people around the table or in the room and having 2 a level of collaboration and honesty around the work 3 that needed to be done, actually resulted in some proper 4 development in technology and some really very exciting 5 new ideas and new directions that we can go in. 6 Q. Since we're discussing it, let's look at it now. 7 I think you deal with that at your paragraph 33, but the 8 chair and panel have already heard about the Hackathon 9 taking place last year. 10 Essentially, as I understand it, at the conclusion, 11 I think, of a two-day brainstorming session, to use your 12 phrase, there was a prototype that was developed -- 13 A. Yes. 14 Q. -- that could potentially be used to flag conversations 15 that might be used and commonly encountered in grooming? 16 A. That's correct. 17 Q. Is there any update that you're able to give us on 18 what's happened with the prototype and where it is going 19 next? 20 A. Yes, so now it's -- we've got this kernel of an idea. 21 We've got some really very exciting directions that we 22 can take this in. We've got the engineers within 23 Microsoft now very committed to driving this forward, 24 and we're making progress on it. 25 I had an update on it a couple of weeks ago, and</p> <p style="text-align: center;">Page 92</p>

<p>1 I think the feeling is that it's getting towards the 2 sort of beta stage of testing. 3 Q. Help me with what that means in layman's terms? 4 A. That really is, how do you start applying it in real-use 5 cases, in order to see how it performs, and what 6 adjustments you might need to make to it in order to 7 improve it further. 8 Q. Is there any timescale or end date by which it's hoped 9 that the prototype will, in fact, be eventually 10 introduced? 11 A. I don't have a date for that. 12 Q. No. 13 A. But we will get it when we -- as soon as we can. 14 Because -- because it's -- the idea is it helps to 15 identify grooming that's taking place, and so, the 16 sooner we can get it in shape, the better. 17 Q. It's not that I want to put Microsoft or any of those 18 involved in the Hackathon under some unrealistic 19 timetable, but one of the things the chair and panel 20 have heard is, talks happen, there's engagement, and 21 then sometimes months, if not years, elapse before 22 there's an end product. 23 I just wondered if there's any way I could press you 24 for what might be anticipated to be a realistic end date 25 for when this prototype may actually be introduced?</p> <p style="text-align: center;">Page 93</p>	<p>1 A. I can't -- I can't give you that, I'm afraid. 2 Q. Are we talking months or years? 3 A. We're talking months. 4 Q. Months. 5 We slightly jumped ahead to deal with the Hackathon. 6 Can I just deal with, please, the remaining sort of 7 budgetary-type questions and look at some of the 8 financial and operational support that Microsoft 9 provides to various organisations. I'm at your 10 paragraph 18 onwards in your statement. 11 You've given evidence about the budget and as much 12 as you can say in relation to that, but in addition to 13 that, is it right that there is also financial support 14 and what you term support in kind for various 15 stakeholders in this area? Just help me with what you 16 mean by "support in kind"? 17 A. So support in kind might be that we gift or loan 18 engineers to help with the integration of various 19 solutions. We might -- a good example is the work we've 20 done with the Internet Watch Foundation where we've also 21 asked for their help and provided a budget to support 22 that around certain aspects where we've wanted to 23 make -- we've wanted to understand the landscape a bit 24 further and develop our thinking better, and so that 25 there has been funding support of that kind.</p> <p style="text-align: center;">Page 94</p>
<p>1 Q. Can I stop you there, because you mentioned the IWF and 2 I think it's in right that, in 2018, Microsoft helped 3 fund research that was being conducted by the IWF -- is 4 that right? -- in relation to examining the distribution 5 of captures of live streamed child sexual abuse? 6 A. Yes, that's exactly the kind of work that we think is 7 both valuable for us and for the organisations that are 8 advancing -- 9 Q. I'd like to have a look at that paper, if I may, but can 10 I just understand, what was the motivation behind 11 Microsoft deciding to fund that research? 12 A. Well, we're concerned about how Skype is used for live 13 streaming of child sexual abuse and we wanted to spend 14 some time investigating further what could be done, what 15 is the -- you know, what interventions would be helpful 16 to be able to address some of the issues that we see 17 from that. 18 And so, this was a direction that we felt was 19 worthwhile. It was also the findings from that that 20 helped us to develop the PhotoDNA for video. 21 Q. Can we have a look at some of the body of the actual 22 research, and, chair, can I invite you, please, to look 23 behind tab B1 and call up on screen, please, 24 IWF000010_004. 25 It might be easier, Mr Milward, just to look at the</p> <p style="text-align: center;">Page 95</p>	<p>1 document that comes up on the screen. 2 Chair, this is not a document that we've looked at 3 previously, so if I can just introduce it in this way. 4 The study was carried out by the IWF, funded by 5 Microsoft, to look at images and videos that were 6 collected over a three-month period in, I think, August 7 to October 2017. 8 During the study, 2,082 images and videos were 9 assessed and the findings are set out -- perhaps if we 10 can highlight the key findings -- because they have 11 an impact on live streaming and who is a victim and 12 potential victim of that form of abuse. 13 The findings were that 96 per cent of the videos and 14 imagery depicted children on their own, typically in 15 a home setting such as their own bedroom. 98 per cent 16 of the imagery was children of 13 years or younger. 17 96 per cent of the imagery featured girls and 18 40 per cent of the imagery was category A or B, so at 19 the more serious end of the categorisation within the 20 UK. 21 100 per cent of the imagery had been harvested from 22 the original upload location and was being redistributed 23 on third-party websites. 4 per cent of the imagery was 24 captured on mobile-only streaming apps and 73 per cent 25 of the imagery appeared on 16 dedicated forums with the</p> <p style="text-align: center;">Page 96</p>

<p>1 purpose of advertising paid downloads of videos of 2 webcam child sexual abuse. 3 Chair, you may recall in opening I said it wasn't 4 just the case then that the live streaming is that 5 coming in from South East Asia, there is also 6 potentially live streaming coming in from western 7 children. 8 It's against that background, Mr Milward, that -- if 9 you turn over the page in your bundle, and if we call up 10 page 18 of the same document, there is a section there 11 that's headed "Development and implementation of new 12 solutions, including video hashing technology to detect 13 captures of live stream child sexual abuse." 14 I hope this might be a section you can help us with. 15 In the middle of that page, there is reference there 16 to: 17 "The use of image hash lists using Microsoft's 18 PhotoDNA are an effective tool to prevent the upload and 19 to detect distribution of duplicates of child sexual 20 abuse images and online services. 21 "Whilst a number of solutions are in development, to 22 date there is no similar industry standard for the 23 detection of duplicative video content. The development 24 of an industry standard method for hashing videos of 25 child sexual abuse would enable videos being</p> <p style="text-align: center;">Page 97</p>	<p>1 redistributed within cyber lockers ..." 2 What is a "cyber locker"? 3 A. It is an encrypted storage facility. 4 Q. "... to be quickly identified and removed. IWF is 5 currently working with Microsoft to develop an industry 6 standard enabling a list of video hashes to be created", 7 and it goes on. 8 I wonder if we can just summarise that, perhaps, in 9 a more public-friendly way. What, essentially, was the 10 outcome, as far as Microsoft was concerned, from this 11 research and where is it intended that Microsoft go 12 next? 13 A. Yes, so what really this showed was -- actually, you 14 probably -- IWF will have a -- it was their research. 15 But, for us, we saw this and we quickly realised that, 16 if you have one single live stream of abuse, that live 17 stream is then captured and then shared on multiple 18 times. 19 And while it was -- it is incredibly, it remains 20 incredibly difficult to stop that one instance of the 21 live stream, that there must be a way -- and I think 22 this report points to it -- of developing technology 23 that tries to address the way in which that live stream 24 is then shared on multiple times. 25 Q. So you can't stop it happening, but you could stop the</p> <p style="text-align: center;">Page 98</p>
<p>1 sharing, potentially? 2 A. In summary. 3 Q. Yes. 4 A. It was this that prompted us to focus more attention on 5 to the development of PhotoDNA for video. 6 Q. Right, I'm going to come on to that as well. 7 Let's look at PhotoDNA then. I think that starts at 8 your paragraph 45. 9 If I may, may we go back to some basics -- 10 A. Yes. 11 Q. -- with PhotoDNA? 12 It was developed in 2009. Why did Microsoft get 13 involved with the development of this software? 14 A. Well, we actually wanted to do something about child 15 sexual abuse and, largely, we became aware of this and 16 the prevalence of this in a conversation in a report 17 from Toronto Police in about 2008, I think. It really 18 focused our attention on this as an issue, and so we 19 started looking around for where there was exciting and 20 progressive development of technologies that might 21 actually address this, which led us to Dartmouth 22 College. 23 Q. Was there a -- really, what I'm trying to understand is 24 why Microsoft decided that they were the ones that 25 should be getting involved in this?</p> <p style="text-align: center;">Page 99</p>	<p>1 A. That's a good question. 2 Q. What's the rationale behind it? 3 A. I mean, I think our feeling was that we didn't want to 4 be a platform of choice for abusers and, equally, for 5 terrorists, put it that way, and so we wanted to ensure 6 that we were making a contribution that tried to ensure 7 that we were, you know, protecting our customers, 8 protecting our users, and that, you know, we would try 9 to -- we're making the effort that they expected of us 10 to -- to create a -- you know, a safer space. 11 Q. Let's look at how it works. 12 It might assist, chair, if we look behind tab 2 and 13 call up on screen MIC000012_003. 14 Now, although, Mr Milward, the chair and panel have 15 heard about hashes a number of times, I want us to try 16 to actually practically understand how PhotoDNA works. 17 This image in the middle -- and the explanation may 18 or may not assist, but it may be useful for some people. 19 Can you just talk us through how PhotoDNA technology 20 works? 21 A. Yes, so put simply, you can take an image and scan it 22 and it effectively turns that image into a string of 23 numbers. 24 Then you can compare that string of numbers with 25 other strings of numbers and, if the string of numbers</p> <p style="text-align: center;">Page 100</p>

<p>1 is similar or the same, then you can reach a conclusion, 2 with very great accuracy, that the image is the same or 3 similar. 4 What I mean by "similar", is that it allows us to 5 identify images, even if there have been attempts to try 6 to adjust the colour saturation of the image or the 7 image has been cropped slightly differently or, indeed, 8 if that image is a still frame from a video and you're 9 comparing it to an image of the next frame on in the 10 video. 11 So it does allow you to identify images, including 12 images that are very similar images. 13 Q. Can I ask you about that, because I just want to try and 14 understand the limits of what is similar or not. 15 If I were to take an image of me now with my glasses 16 on and I were to take them off, would PhotoDNA be able 17 to recognise me with my glasses off? 18 A. Well, it's not -- it's not facial recognition. 19 Q. I understand that. 20 A. It's not AI-driven, it's about -- it will be on a -- it 21 will be on a sliding scale. So depending on how 22 different you look with your glasses off, it would 23 determine -- but it would also take into account not 24 just you, it would look at the pillar behind you, the 25 clothes that you are wearing, your necklace, your hair</p> <p style="text-align: center;">Page 101</p>	<p>1 other aspects that then might determine, if you took 2 your glasses off, that was sufficiently similar with all 3 other aspects of the image that it was, therefore, 4 similar. 5 Q. So it doesn't have to compare identical images, there is 6 a margin of appreciation, but it might depend on 7 a number of factors how wide that margin is? 8 A. That's right, and that's also part of its value. 9 Once the image has been hashed, it goes into, 10 I think -- is it a database containing the hashes? 11 A. Yes, there are two hash databases. One is managed by 12 IWF and one by NCMEC. 13 Q. And then the database, do you -- is it maintained and 14 updated, is that done by NCMEC and the IWF? 15 A. Yes. So the idea is that every user of PhotoDNA -- and 16 there are roughly 155 and -- and counting. I mean, we 17 welcome more. I think NCMEC licenses it for use. 18 I think IWF also contributes to, you know, ascertaining 19 whether other organisations are suitable for using it, 20 but the idea is that all those users of PhotoDNA 21 contribute the hashed images to the hash databases and 22 that way the database continually grows and it means 23 that the PhotoDNA platform is then more and more useful 24 in identifying known images. 25 Q. I think you go on to say that Microsoft have made</p> <p style="text-align: center;">Page 102</p>
<p>1 PhotoDNA available as a service on Azure. What is 2 Azure? 3 A. Azure is our cloud platform and I think the simplest way 4 of thinking about that is that you don't need to install 5 a software package called PhotoDNA in order to operate 6 it. Actually, it can be run from the cloud, which means 7 that you've got -- it's far faster, so in terms of 8 processing, it's almost instantaneous. It means that 9 an organisation can use it and deploy it without any 10 real infrastructure. 11 Q. I think you therefore say it enables smaller companies 12 and organisations to have that capacity if they want to? 13 A. That's right. 14 Q. To date, you say, Microsoft has provided PhotoDNA 15 technology to more than 155 organisations. You've also 16 made PhotoDNA available to law enforcement worldwide? 17 A. That's correct. 18 Q. Is there any charge for that service? 19 A. No, there's no charge. 20 Q. Why have Microsoft given that away free of charge? 21 A. It was the right thing to do. This technology is 22 designed to try to identify and remove these images. To 23 charge for it is -- would've been the wrong decision. 24 Q. Has PhotoDNA now evolved to cover still images and 25 videos? Have I got that right?</p> <p style="text-align: center;">Page 103</p>	<p>1 A. Yes, so this is the next development of PhotoDNA, which 2 is that we've been able to move the engineering on 3 further and -- and PhotoDNA -- PhotoDNA for video can 4 then -- it can identify entire videos or sections of 5 video and match them to known abuse videos. 6 Q. Can we call up, please, and you look behind tab 3 in 7 your bundle, MIC000018_003. 8 There's a similar diagram explaining how PhotoDNA 9 video works. 10 Again, can I just ask you to talk us through, as 11 simply as you're able to, how it works now with video? 12 A. It's pretty much identical, in terms of it will take 13 a section of video and it will hash it, and then it can 14 allow the -- that hash then can be matched against other 15 hashes to identify a known sexual abuse content. 16 Again, the important thing to note here is that it 17 will match against known content. 18 Q. Yes. Yes. 19 I'm going to come on to deal with unknown content. 20 A. So the -- the way in which it will improve is that the 21 number of hashes, so the richness of the hash database, 22 and the number of PhotoDNA users that -- that we have 23 using the platform. 24 Q. Is PhotoDNA video also made available to those 25 organisations on Azure to law enforcement?</p> <p style="text-align: center;">Page 104</p>

<p>1 A. Yes, it is.</p> <p>2 Q. And again for free?</p> <p>3 A. For free.</p> <p>4 Q. The PhotoDNA covering the cloud, is that only covering</p> <p>5 still images, not videos?</p> <p>6 A. Sorry, could you clarify your question?</p> <p>7 Q. I was looking at your paragraph 47, which deals with the</p> <p>8 availability of PhotoDNA on Azure or the cloud services,</p> <p>9 and just wondered whether that -- any video that was</p> <p>10 uploaded to the cloud, would PhotoDNA still operate on</p> <p>11 the cloud?</p> <p>12 A. Yes, yes, so -- so PhotoDNA for video also operates in</p> <p>13 the cloud, yes.</p> <p>14 Q. Thank you.</p> <p>15 Looking at your paragraph 50, I think you said this:</p> <p>16 "In 2016, Microsoft provided the IWF with</p> <p>17 sublicensing rights to PhotoDNA to enable IWF members to</p> <p>18 access the IF Image Hash List, deployed through the</p> <p>19 PhotoDNA cloud solution."</p> <p>20 A. Yes.</p> <p>21 Q. What, in practice, does that mean?</p> <p>22 A. So effectively it means that IWF has the knowledge and</p> <p>23 expertise to determine whether a company or</p> <p>24 an organisation really is qualified or should be using</p> <p>25 this sort of technology in the fight against child</p> <p style="text-align: center;">Page 105</p>	<p>1 sexual abuse. We felt that -- we have strengths in lots</p> <p>2 of areas, but IWF is really expert in this.</p> <p>3 Q. Can I ask you please to look behind your tab 4 and we</p> <p>4 call up on screen MIC000019_002. This is a report taken</p> <p>5 from the IWF dated October 2016, when I think this</p> <p>6 matter was resolved and the hash list was made</p> <p>7 available.</p> <p>8 Just looking at the technical details at the bottom</p> <p>9 of the page, this might explain it more easily:</p> <p>10 "The IWF and Microsoft have teamed up to make it</p> <p>11 easy for companies to use the Image Hash List.</p> <p>12 Microsoft PhotoDNA has been the industry standard since</p> <p>13 2009 and previously companies had to integrate hashes</p> <p>14 internally, often incurring high costs due to extensive</p> <p>15 engineering.</p> <p>16 "From today, the Microsoft and IWF collaboration has</p> <p>17 allowed a cloud-based delivery solution. The obstacles</p> <p>18 of in-house engineering have been removed, meaning that</p> <p>19 proactive monitoring of a company's platform is no</p> <p>20 longer just for the big industry members."</p> <p>21 "Companies can compare anything from a single image</p> <p>22 to the millions of images uploaded through their</p> <p>23 platforms daily, using the cloud solution. For most</p> <p>24 companies, it's not possible to manually scan every</p> <p>25 image which is uploaded onto their platforms as the</p> <p style="text-align: center;">Page 106</p>
<p>1 numbers are too high. So the IWF Image Hash List</p> <p>2 deployed, deployed through the cloud solution, can do it</p> <p>3 for them.</p> <p>4 "Companies can do all of this without affecting the</p> <p>5 users' experience due to the speed and efficiency of the</p> <p>6 cloud solution. Any IWF member can integrate the cloud</p> <p>7 solution into their platform and be proactive in</p> <p>8 monitoring against the distribution of online child</p> <p>9 sexual abuse."</p> <p>10 So, essentially, to avail oneself of this technical</p> <p>11 advancement, you have to be an IWF member?</p> <p>12 A. No, you don't have to be.</p> <p>13 Q. That's what I wanted to be clear about.</p> <p>14 A. Yes, and so I mean there are a range of organisations</p> <p>15 all over the world who are using this. You know, some</p> <p>16 of them are IWF members, including Facebook, Google,</p> <p>17 Twitter, Yahoo and others. But you don't have to be.</p> <p>18 I think IWF can help us to identify others who might be</p> <p>19 able to use this to good effect.</p> <p>20 Q. Just finally dealing with PhotoDNA, at paragraph 51 you</p> <p>21 say:</p> <p>22 "Microsoft has provided PhotoDNA for free to any</p> <p>23 qualified organisation..."</p> <p>24 A. Yes.</p> <p>25 Q. What's a "qualified organisation"?</p> <p style="text-align: center;">Page 107</p>	<p>1 A. Now I'm scratching my head a little bit about that as</p> <p>2 well. The honest truth is that a qualified organisation</p> <p>3 is an organisation that can actually make use of it, and</p> <p>4 isn't going to be trying to reverse-engineer the</p> <p>5 technology or to be able to use it for any other aims</p> <p>6 for what it's not -- that's not its purpose. So it</p> <p>7 really is for organisations that are determined to try</p> <p>8 to use this in order to, you know, kind of join the</p> <p>9 fight against child sexual abuse material being shared</p> <p>10 on the internet.</p> <p>11 Q. Before we break this afternoon, now that we've</p> <p>12 considered how PhotoDNA works, just consider its impact</p> <p>13 in relation to indecent images of children. Can I ask</p> <p>14 you, please, to look at your paragraph 25 in your</p> <p>15 statement onwards.</p> <p>16 A. Yes.</p> <p>17 Q. And some of the things that Microsoft have been doing in</p> <p>18 relation to indecent imagery, including self-generated</p> <p>19 images.</p> <p>20 I think you said that:</p> <p>21 "Microsoft uses a range of hashing technologies to</p> <p>22 identify and remove such material from its platforms and</p> <p>23 services."</p> <p>24 And for the Bing search engine, Microsoft uses the</p> <p>25 IWF hash list, which we've just discussed.</p> <p style="text-align: center;">Page 108</p>

1 **A. Yes.**
 2 Q. And other databases. Would that include the NCMEC
 3 database?
 4 **A. That does.**
 5 Q. To ensure that child abuse imagery doesn't appear in the
 6 search results.
 7 Microsoft has made an average of 5,800-monthly
 8 reports to NCMEC over the last 40 months. So your
 9 statement, I think, was dated December 18, so it's about
 10 from the summer of 2014 to December 18. 5,800, is that
 11 per month?
 12 **A. Per month.**
 13 Q. Has that figure remained roughly constant from 2014
 14 through to December 2018?
 15 **A. I think that we've seen an increase in the number of**
 16 **referrals we've made, but it's been broadly -- that's**
 17 **broadly right. If you think about the number of**
 18 **referrals NCMEC receives has gone from around 17 million**
 19 **last year, 10 million the year before, and that 10**
 20 **million was a larger number than all previous years. So**
 21 **you've seen a significant increase in the numbers of**
 22 **images that are being reported to NCMEC.**
 23 That doesn't mean that we can't -- we can't draw
 24 a firm line between the number of images that are
 25 reported and the increased incidents of child abuse,

Page 109

1 a platform for sharing abuse, is really, you know, it's
 2 very limited and it's limited to pretty much the gamer
 3 tag. So that is if you are playing a game on Xbox,
 4 you'll have your gaming name which might be, you know,
 5 I don't know, what, "cool dad 57", or something, you
 6 know, it's a gaming name, and you have the option of
 7 putting a little image of yourself or a little image on
 8 it. And what we're finding is that predominantly on
 9 Xbox we're finding that those little images that people
 10 load up are child sexual abuse images. That's
 11 an example of where these are surfacing on Xbox as
 12 a platform.
 13 So actually, in terms of the number of images we
 14 find across our platforms, it's actually -- it's pretty
 15 limited.
 16 Q. The 5,800 figure, as I understand it, is a global
 17 figure?
 18 **A. That's correct.**
 19 Q. I think you say it is not possible to provide specific
 20 figures for the UK.
 21 Why is it not possible to provide a national figure?
 22 **A. So we don't always know from where the referral to NCMEC**
 23 **ultimately comes from. Particularly in our consumer**
 24 **platforms, a lot of the data is located in the US, and**
 25 **it's very difficult to identify, you know, ultimately**

Page 111

1 because part of the reason for that increase is because
 2 more organisations are using technologies like PhotoDNA,
 3 and more organisations, that more companies and
 4 individuals are aware, and aware of their responsibility
 5 to both report it and to deal with it and have made
 6 themselves, you know, given a greater understanding of
 7 what NCMEC will do and have -- actually kind of raise
 8 their game in terms of the fight against child sexual
 9 abuse.
 10 So we can't say for certain that the incidences of
 11 child abuse have gone up, but we can say for certain the
 12 number of reports have definitely gone up.
 13 Q. Given what is, on any view, that when we are talking
 14 about the millions of referrals to NCMEC, an
 15 extortionate rise between 10 million and 17 million,
 16 I just was curious to see how that fits in with the
 17 roughly 5,800 reports, which seems a relatively constant
 18 number across Microsoft. Do you have any understanding
 19 of why it's seemingly constant at Microsoft's level of
 20 reporting and yet, at the other end, at NCMEC, there is
 21 such a large rise? Your detection rates have
 22 potentially sort of stayed roughly the same.
 23 **A. Well, it's either the detection rates, or that actually**
 24 **Microsoft is not the platform of choice for this kind of**
 25 **sharing of abusive images. You know, Xbox Live, as**

Page 110

1 where it's actually come from. Similarly, with the
 2 cyber tips that are made to NCMEC, they do identify the
 3 location of where the abuse took place because that's
 4 the mechanism by which law enforcement can then follow
 5 up.
 6 Q. Yes.
 7 **A. But we can't go -- it's not possible to go into the**
 8 **granular detail around those 5,800 exactly, which**
 9 **countries they're all from.**
 10 Q. So it's not possible to get any sense out of that 5,800
 11 at all, which of that relates to the UK?
 12 **A. It's not. We don't -- so we could re-engineer the data**
 13 **that we collect and be able to report out, but at the**
 14 **moment we don't do that.**
 15 Q. Why not?
 16 **A. I think that it -- you know, we think about the way in**
 17 **which we're tackling this in every country, and we want**
 18 **to make a difference in every country. So breaking it**
 19 **down for the UK, or for any other particular country, it**
 20 **really -- it doesn't help us in the fight that we're**
 21 **making, that it ... Yeah, I mean I can -- I might have**
 22 **to come back to you with some more information about,**
 23 **you know, precisely how we might do this and why we**
 24 **haven't made this decision before.**
 25 Q. Before we break may I ask you about one other topic.

Page 112

<p>1 I would like you to turn, please, in tab 5 in the 2 bundle, chair, and call up on screen INQ004187_001. 3 Mr Milward, this is an article that appeared in The 4 Telegraph in January of this year with the headline 5 "Microsoft search engine Bing shows child pornography, 6 report finds". I know that you have looked at this and 7 also provided a second statement; if you need to refer 8 to that second statement, please do. 9 But just so that everyone who is following, if we 10 can turn to the second page of the reference, please. 11 Perhaps if we -- thank you very much. 12 The article read: 13 "Microsoft's Bing is allowing child pornography 14 images to appear in its search results and is aiding 15 paedophiles by suggesting other terms they could search 16 for. 17 "An investigation by AntiToxin, an online safety 18 company, found multiple cases of the illegal images 19 showing up in the search engine's results. 20 "The search engine had the illegal images in results 21 when terms such as 'porn kids' or 'nude family kids' 22 were typed into Bing. 23 "The site's search suggestions also directed the 24 researchers to child pornography. For example, the term 25 'Omegle Kids', referring to a video chat app that is</p> <p style="text-align: center;">Page 113</p>	<p>1 popular with children, suggested the search 'Omegle Kids 2 Girls 13' which produced illegal imagery. 3 "Another search for 'Omegle for 12 year old' 4 prompted Bing to suggest searching for 'Kids on Omegle 5 Showing' which led to illegal images. 6 "Bing would also show users additional explicit 7 pictures of children through its 'similar images' 8 feature." 9 Can I just break down to those various points in the 10 article to just understand what it was that AntiToxin 11 found and then ask what Microsoft did about it. 12 A. Yes. 13 Q. Taking each in turn, the first suggestion is that the 14 search engine had illegal images in results when terms 15 such as "porn kids" or "nude family kids" were typed 16 into Bing. 17 Firstly, do you accept the findings of what 18 AntiToxin reported here as uncovering? 19 A. Well, we spent some time trying to replicate the 20 results. I think there is some debate as to, you know, 21 in terms of the 4x4 grid, how these particular images 22 might classify. 23 Q. Right. 24 A. I think, you know, it kind of gives a very clear example 25 of why automating or applying AI to the determination of</p> <p style="text-align: center;">Page 114</p>
<p>1 what is a child or what is a person of a particular age 2 is very risky, because it's not a precise art and it's 3 a challenge. 4 So whilst it's debatable as to where on that 4x4 5 grid these images actually appeared, what was really 6 clear was that, in any event, the results that came up, 7 when you search for them, were not good enough, and so 8 we needed to act. 9 Q. Do I take it that the searches, when they did come up, 10 were clearly not of known or hashed child abuse imagery 11 otherwise PhotoDNA would have presumably operated in 12 such a way as to ensure that they weren't detected? 13 A. I think that's a good assumption, but I mean again it 14 depends on whether those images have been classified as 15 child sexual abuse material through PhotoDNA. 16 Q. The article goes on to deal with what search terms were 17 put in. 18 A. Yes. 19 Q. I want to make sure that everyone understands that 20 properly. If the search term "Omegle Kids" was put in, 21 as you know, once you start typing out "Omegle" it might 22 go on to provide an additional word or additional two or 23 three words. What actually happened here as far as 24 Microsoft is aware when one started to type, for 25 example, the term "Omegle Kids"?</p> <p style="text-align: center;">Page 115</p>	<p>1 A. So what we have found is some aspects of search that 2 have prompted us to take a slightly -- a fresh look in 3 a new direction in the way that we think about search. 4 And that is largely because some terms that are very 5 common terms were effectively delivering what we would 6 say as being suboptimal results, or results that were -- 7 that you shouldn't -- that you shouldn't expect to be 8 appearing according to those terms. 9 Other terms -- 10 Q. Could you give us an example. 11 A. So, for example, you have search terms that are clearly 12 intent, search terms with intent. Now, if you search 13 for "porn kids" -- 14 Q. Yes. 15 A. -- you're clearly searching with the intent to identify 16 pornography relating to children. 17 So, you know, our focus on how do you respond to 18 search terms with very clear intent? And it should 19 be -- nothing should be appearing on that. And things 20 were appearing on it, and so it prompted us to take 21 a different direction. 22 There are other search terms like "Omegle Kids" that 23 it's very difficult to determine whether that is 24 a single intent search. It's safe to say that there 25 are, every day, millions of search queries that are put</p> <p style="text-align: center;">Page 116</p>

1 into a search engine, including Bing, that have never
 2 been searched for before. So effectively the search
 3 engine hasn't got a history or a precedent of how to
 4 respond to that particular search, and so it looks for
 5 other things, and that's where it starts doing things
 6 like suggesting wording and taking into account previous
 7 searches or searches immediately before, and then trying
 8 to find, well, what was this user really trying to
 9 discover on the internet?
 10 You know, and so what it has done is it has prompted
 11 us to think much more carefully about, instead of just
 12 focusing on search terms that it was very clear what the
 13 intent was and we shouldn't be serving results against
 14 their intent, and the other end of the scale, search
 15 terms that were deliberately masking and, you know, had
 16 dual intent, and therefore, you know, you could surface
 17 images that were child sexual abuse images or images
 18 that had nothing to do with it. You know, a good
 19 example is the sort of search terms that might result in
 20 either an academic paper, or a news report, or in fact
 21 the findings of this inquiry, and what else might
 22 surface in those same results.
 23 Actually we've been too focused on either end of the
 24 scale. What we've done is we've missed the sort of grey
 25 area that sits in between. What this investigation

Page 117

1 organisations that chair and panel are no doubt familiar
 2 with, and indeed why is it, when there's all this
 3 collaboration, nonetheless we still end up in 2019,
 4 in January of this year, with results being brought back
 5 and potentially illegal images being uncovered on
 6 a search? If you're part of it, it might suggest that
 7 the collaboration is either perhaps a talking shop or is
 8 perhaps not as effective as everyone was led to believe?
 9 **A. No, I think it's because this whole thing is not**
 10 **a destination really, it's a journey. The abusers and**
 11 **those who are determined to share and view these kind of**
 12 **images are constantly finding new ways in which they can**
 13 **mask their tracks or to effectively fool the algorithm**
 14 **when it comes to search. So the introduction of things**
 15 **like exclamation marks and other bits of punctuation**
 16 **into a search term, which we've never really seen before**
 17 **-- and we're not talking about boolean search, we're**
 18 **talking about using punctuation in the search term --**
 19 **then actually it's all designed to try to gain the**
 20 **algorithm, to try to surface what is out there on the**
 21 **internet.**
 22 **Bear in mind that the search engine crawls -- it**
 23 **doesn't host, it doesn't host any content -- it crawls**
 24 **the internet to discover what is out there on the**
 25 **internet that is publicly available. Then it surfaces,**

Page 119

1 prompted us to do was to fundamentally sit down and
 2 re-think the way in which we were devoting engineering
 3 attention to the challenge that we face here.
 4 So actually it's largely as a result of AntiToxin
 5 and IWF that we've worked to actually make quite
 6 a significant change in the way that we're thinking
 7 about the way that search responds to these kind of
 8 queries.
 9 Q. The article was written in January 2019, and one might
 10 want to know why it took an exposé such as this to have
 11 Microsoft re-think its approach to auto-suggested search
 12 terms. Why does it take a publicity such as this to
 13 cause a re-think by Microsoft in terms of child safety?
 14 **A. It's a good question, and what I do think this points to**
 15 **is the value of having other organisations working with**
 16 **us on this kind of thing, you know. The ability of the**
 17 **IWF to help us think through, you know, how we approach**
 18 **this, the ability of campaigning organisations, NGOs,**
 19 **journalists, to hold us to account over this kind of**
 20 **thing is incredibly important. You know, it's that**
 21 **collective action that we're going to see incremental**
 22 **improvements in the way that these kind of things work.**
 23 Q. It's not a counsel of perfection, but given that
 24 Microsoft sits on the IWF, collaborates with NCMEC, is
 25 a member of WePROTECT, INHOPE, all the other

Page 118

1 **links, to the results of what it finds.**
 2 **You know, this not a human-moderated function, it is**
 3 **an algorithm that says, in response to this kind of**
 4 **query, "that looks like that little bit over there of**
 5 **the web". Bear in mind the number of web pages uploaded**
 6 **or adjusted every day, you know, the challenge is to**
 7 **stay ahead of those people who are trying to gain the**
 8 **search algorithm.**
 9 MS CAREY: Chair, I wonder if that would be a convenient
 10 point to stop for today's session.
 11 THE CHAIR: Thank you very much.
 12 (4.05 pm)
 13 (The hearing adjourned until
 14 Thursday, 16 May 2019 at 10.30 am)
 15
 16
 17 I N D E X
 18
 19 (In Open Session)1
 20 MS MELISSA MARRUS POLINSKY1
 21 (affirmed)
 22 Examination by MR KRISHNAN1
 23 (The court went into closed session)71
 24 (In Open Session)71
 25 MR HUGH CHARLES MILWARD (affirmed)72
 Examination by MS CAREY72

Page 120

A	academic 117:20	acts 36:14	Agency's 89:15	16:13 61:2
A1 1:16	accept 5:22 45:17 59:10 114:17	actual 24:16 28:7 95:21	aggregate 89:12	anticipated 93:24
ability 18:14 24:6,8 35:13 68:4 73:6 118:16,18	accepts 5:22	add 20:11	ago 29:23 92:25	anticipation 60:24
able 5:8 18:15 26:3 27:15 29:11 32:7 32:13 33:14 36:23 49:8 58:8 66:15 68:10,11 69:15 73:13 77:8 81:6 82:10 85:9 87:1 87:16 92:17 95:16 101:16 104:2,11 107:19 108:5 112:13	access 4:4,18 5:15 9:20 29:3 30:19 30:25 32:13 33:8 33:19 34:6 36:23 37:21,22 44:6 49:1,7 73:6 82:14 82:16,19,20 83:14 84:4 85:9 105:18	addition 18:4 85:2 94:12	agree 81:25	AntiToxin 113:17 114:10,18 118:4
absolute 83:11	accessible 39:1	additional 11:12 20:11 29:16 69:9 69:12 114:6 115:22,22	Ah 29:1 51:25	APL000014 50:24
absolutely 2:12 9:1 19:12 36:21 37:5 37:15 38:14 44:23 58:17 82:16 84:13	account 29:2,3,4 30:16,17 41:16 42:1 50:8,10 51:17,18,22 52:9 52:10,11,18,20,22 52:24 54:10,13,17 55:8,16,24,25 56:8 57:4,6,16 58:9 82:13,15 83:16 101:23 117:6 118:19	address 5:19,20 14:21 32:25 37:8 37:8 52:4 95:16 98:23 99:21	ahead 94:5 120:7	apologise 33:3 34:21 43:7 44:11 51:10
abstract 34:21 69:13	Account-based 52:2	addresses 42:4,5 54:22	AI 86:17,22 89:1 114:25	app 4:3 9:2,4,4,5,6 9:13,14,15,16,16 9:18,21,21 10:5,5 10:14 18:22,22,25 19:2,3,7,10,17,18 19:19,23,24,25 20:1,2,2,3,4,5,7,9 20:10,12,17,21,25 21:9 22:5,9,13,20 23:3,4,6,7,16,20 34:16 61:19,20,22 62:10,18,22,23 63:4,5 113:25
abuse 8:19 10:15 20:18 21:13 26:6 31:1 35:7,24 36:18 37:1 39:24 63:17 65:10 67:11 70:7 75:4 77:4 79:7 80:16 81:23 82:1,2,12,25 84:22 85:17 86:12 86:24 87:9,24 88:3,10,15 95:5 95:13 96:12 97:2 97:13,20,25 98:16 99:15 104:5,15 106:1 107:9 108:9 109:5,25 110:9,11 111:1,10 112:3 115:10,15 117:17	accounts 50:11 51:23 52:3,9	adjoined 120:13	AI-driven 101:20	appeal 83:13
abused 40:24	accuracy 101:2	adjourned 120:13	aiding 113:14	appeals 83:15
abusers 100:4 119:10	accurate 66:16 82:7,8	adjournment 71:18	aims 108:5	appear 55:6 109:5 113:14
abusive 110:25	achievable 59:25	adjust 101:6	akin 37:5	appeared 96:25 113:3 115:5
	achieve 26:12	adjusted 120:6	alert 22:2	appearing 75:22 116:8,19,20
	act 45:12 46:16,17 46:18,20,24 47:6 115:8	adjustments 93:6	alerted 21:24 23:15	appears 10:9
	action 82:10 118:21	adult 9:12 22:17 73:6	algorithm 119:13 119:20 120:3,8	Apple 1:7,22 2:18 3:4,7,24,25 4:1,5 4:6,7,9,15,18,21 6:16,24 8:19 10:20 12:2,5 13:2 14:21 15:8,23 17:21 18:6 19:15 22:12,21,23 25:3 25:7,13 26:4 28:4 28:6,20,24 29:2,3 29:4,4,6,11,19 30:12 31:2,3 32:1 32:2,7,18 33:13 34:4 35:8,19,24
	active 6:17	adults 2:16	allow 4:25 101:11 104:14	
	actively 15:20	advancement 107:11	allowed 21:22 106:17	
	activities 36:11	advancing 95:8	allowing 113:13	
	activity 9:11 17:9 19:22 37:16 87:12 88:13	advantage 68:3	allows 3:22 77:18 77:21 101:4	
	actor 80:10	advertising 97:1	amazing 39:12	
	actors 39:15	affairs 59:21 72:8 72:13 86:4	America 67:16 83:22	
		affirmed 1:9 72:1 120:20,24	amount 24:11 78:19 81:15 89:23	
		afraid 24:21 94:1	analysed 81:14	
		afternoon 71:13 108:11	analyses 81:18	
		age 5:5,25 66:4 70:19 84:9,11 115:1	analysis 82:6	
		agencies 28:23 29:1 48:21 49:19 58:23	analysts 8:12 80:2 85:24	
		agency 15:19 45:8 45:9 46:2 53:5,21 54:10 59:20 90:2 90:23	and/or 38:24	
			announced 66:7	
			annual 87:20	
			answer 29:17 30:3 30:3 34:21 36:9 40:12 42:2 44:15 54:14 57:17 69:16	
			answers 37:20 42:3 58:7	
			anticipate 11:21	

38:12 39:20 41:23 42:13,18 43:16 46:13 47:5,11 49:1,7,20,24 50:12 51:6,23 53:11,24 54:4,7 54:10,24 55:17,21 56:4 57:25 58:13 58:14 59:9,13 62:10,16,21 63:10 63:15,18 64:4,19 65:8,11,12 69:23 70:10 Apple's 3:12,14 6:14 8:23 11:22 14:24 16:14 19:3 26:7 33:18 35:23 36:24 48:22,23 60:7,10 61:16 65:14,17 66:25 68:11 apple.com/families 24:19 25:10 AppleCare 25:19 25:22 application 9:15 applied 48:14 86:20 89:25 applies 32:14 43:14 54:4 apply 37:11,20 46:12 83:25 applying 93:4 114:25 appreciate 52:7 58:7 68:19 69:1,5 69:15 appreciation 102:6 approach 12:5 13:21 18:3 26:7 26:10 48:23,23 63:10 65:12,19 118:11,17 appropriate 61:12 62:19 65:1 71:12	approximately 6:15 8:8 16:5 47:21 apps 4:4 9:7,8,17 19:5,6,10,14,16 19:22 20:12,13,14 21:1,4,5,16,17 22:11,21,24 23:12 23:14,14 24:8,10 42:12 61:20,23,25 62:3,9,12,18 63:1 63:2,3 71:4 96:24 April 59:21 area 29:15 32:21 33:3 43:20 44:15 50:7 53:17 70:17 87:1 89:18,25 94:15 117:25 areas 18:20 87:25 106:2 arises 27:6 arrangements 73:10 arranges 89:20 art 115:2 article 113:3,12 114:10 115:16 118:9 artisanal 13:17 ascertainable 84:17 ascertaining 102:18 Asia 97:5 aside 88:17 89:4,18 asked 27:18 70:19 94:21 asks 60:4,6 68:6 89:16 aspects 40:3 74:24 86:18 87:8 88:9 94:22 102:1,3 116:1 assertion 34:9 59:23 64:14	assess 82:2 assessed 81:13 96:9 assesses 53:24 assessment 53:11 assist 25:23 40:16 87:1,4 100:12,18 assistance 25:18 29:11,14 31:3 32:18 35:8 41:23 42:13 67:21 assists 87:3 assume 31:21 32:14 37:11 50:9 73:18 75:14 Assuming 44:12 assumption 56:1,1 115:13 attack 39:2 87:15 attacks 80:14 attempt 20:3 67:10 attempting 20:10 attempts 101:5 attended 91:7,24 attention 8:23 99:4 99:18 118:3 attests 73:9 attorney 8:5 Attorney's 2:13,14 attributed 55:9,14 August 96:6 auto-suggested 118:11 automatically 31:12 automating 114:25 avail 107:10 availability 105:8 available 19:10 30:4,12,16,20 32:22,23 34:4,11 41:25 48:12 63:14 90:4 103:1,16 104:24 106:7 119:25 avenues 32:22	average 109:7 aware 15:8,11 63:5 73:15 83:2 89:14 99:15 110:4,4 115:24 Azure 103:1,2,3 104:25 105:8 <hr/> B <hr/> B 96:18 B1 50:22 95:23 B2 59:17 back 3:17 21:22 29:17 30:23 32:4 33:5 34:9 42:12 42:23 43:25 48:7 54:12,17 56:2 62:17 71:13 99:9 112:22 119:4 back-ups 34:4 37:24,25 42:3 48:19,20 49:3,3 background 7:23 8:13 97:8 backup 31:6,10,20 31:21 backups 52:6 bad 39:15 baked 26:9 balance 39:20 base 40:4 based 3:1 7:2,12 11:17,17,17,19 43:3 63:1,2 73:17 75:14 79:20 83:18 83:20 bases 53:4 basic 59:8 basically 34:17 45:9 basics 99:9 basis 46:2 53:7,12 82:9,9 bear 84:21 119:22 120:5	bearing 82:13 Beauchere 74:5 bedroom 96:15 behalf 59:19 80:10 believe 5:7 6:2 13:4 15:19 18:10 21:14 21:16 24:13 26:11 35:21 43:5 46:6 46:25 47:2 50:5 51:20 55:23,25 56:18 61:17 62:6 62:8 64:22,25 66:18 68:23 119:8 benefit 70:2,3 best 3:16 24:21 42:24 44:16 50:8 63:3 beta 93:2 better 24:1,2 29:21 66:15 67:20 69:3 83:6 85:14,15 93:16 94:24 beyond 42:11 43:7 big 13:18 106:20 biggest 29:24 30:2 30:5 58:19 billion 6:17 89:23 90:3 billions 11:22 Bing 74:17,18 78:1 78:3,5,9,11,17 108:24 113:5,13 113:22 114:4,6,16 117:1 bit 2:10 4:14,14 5:12 6:4,5,18 17:19,20 18:18 26:25 31:25 33:5 34:20 36:14 56:19 71:13 72:18 73:14 73:22 88:2 91:4 94:23 108:1 120:4 bits 119:15 blackout 18:16 blanketing 67:1
---	--	--	---	---

bleed-over 88:12	business 3:8 13:1 27:3 63:25 65:5 72:13,18	categories 3:11 29:5 53:4	52:20,23,25 54:13 54:15 56:9 57:5	87:9,24 88:3,9,15 95:5,13 97:2,13 97:19,25 99:14 105:25 107:8 108:9 109:5,25 110:8,11 111:10 113:5,13,24 115:1 115:10,15 117:17 118:13
block 84:6,12	businesses 8:5 12:14	categorisation 96:19	challenges 29:24	child's 18:15 24:2,3 24:18 69:3
body 95:21	buy 71:7	categorise 56:23	change 31:9 33:17 33:18 118:6	child-related 58:25
boolean 119:17		category 10:15,21 11:10 14:25 53:19	changing 31:11	children 2:16 12:10 12:18,25 13:2,7 13:16 14:8 15:14 17:22 18:7,11 26:14 38:25 39:23 40:2,17 41:4 61:15,24 62:7 63:6 66:13 69:7 70:21 71:7,10 77:5,7 79:6 84:9 96:14,16 97:7 108:13 114:1,7 116:16
botnet 80:6,7	C	category 10:15,21 11:10 14:25 53:19	channel 36:20	children's 40:18,25 41:2,4 73:5
botnets 80:5		54:7 61:19,23,24 62:1,3 96:18	channels 36:2,3 61:5	China 7:10 57:2,5 57:13
bottom 56:5 58:6 106:8	calculate 27:21	cause 118:13	characterisation 64:11	choice 100:4 110:24
Brad 74:7	calenders 52:6	cent 57:8,10,14 58:4,7 90:7 96:13 96:15,17,18,21,23 96:24	charge 103:18,19 103:20,23	choose 24:8 90:10 90:11
brainstorming 91:20 92:11	California 7:14	central 39:8	Charles 72:1,5 120:24	chose 27:21
break 48:1,5 71:12 108:11 112:25 114:9	call 3:13 16:2 21:10 25:20 60:4 89:17 95:23 97:9 100:13 104:6 106:4 113:2	centralised 42:18 79:23	chat 5:21,23 9:25 21:2 36:2,8,8 113:25	circle 30:23
breaking 112:18	called 69:1 78:1 103:5	Centre 15:14 25:19	check 5:8 6:1 48:16 56:2	circulated 17:4
briefly 3:4 8:24 15:9 17:21 44:21 51:18 53:2 58:15	Cambridge 86:16 86:21	certain 16:23 22:13 22:15 23:14 52:4 55:23 64:16 68:2 78:19 79:2 81:15 87:16 94:22 110:10,11	chief 74:4	circumstance 32:15 82:24
broad 53:20,25 54:5	campaigners 73:5	certainty 26:1 32:23 33:1 34:10 34:13,18 35:1 47:4 62:23 64:21 71:6	child 1:24,25 2:8,15 2:16,17,21 8:1,1,4 8:4,6,19 9:10,24 9:25 10:2,4,6,8,10 10:15,16,25 11:11 12:5,7,12 13:21 13:24 14:20 15:11 15:20 18:3,4,21 18:23 20:18,22 21:11,13 22:14,16 22:25 24:9,11,11 26:5,7 27:3,19 28:3,5 30:9,9 35:8 39:11 42:10 45:23 46:3,4,8 58:24 60:18,20 63:19,24 64:4,23 65:10,16 65:18,24 66:1,2,4 66:4,18,24 67:4 67:17 70:7,10 71:7 75:4 79:7 80:15 81:23 82:1 82:12,25 84:22 85:16 86:12,24	circumstances 22:13 45:17,20 46:12 48:11 55:20 83:2
broader 65:17	campaigning 118:18	chain 13:3 37:9 40:3 64:10 65:23	child 1:24,25 2:8,15 2:16,17,21 8:1,1,4 8:4,6,19 9:10,24 9:25 10:2,4,6,8,10 10:15,16,25 11:11 12:5,7,12 13:21 13:24 14:20 15:11 15:20 18:3,4,21 18:23 20:18,22 21:11,13 22:14,16 22:25 24:9,11,11 26:5,7 27:3,19 28:3,5 30:9,9 35:8 39:11 42:10 45:23 46:3,4,8 58:24 60:18,20 63:19,24 64:4,23 65:10,16 65:18,24 66:1,2,4 66:4,18,24 67:4 67:17 70:7,10 71:7 75:4 79:7 80:15 81:23 82:1 82:12,25 84:22 85:16 86:12,24	cities 7:10
broadly 109:16,17	capacity 103:12	chair 1:4,7 47:25 48:2,3 70:13,15 71:11,15,16,23 79:18 91:3 92:8 93:19 95:22 96:2 97:3 100:12,14 113:2 119:1 120:9 120:11	chat 5:21,23 9:25 21:2 36:2,8,8 113:25	citizen 46:21
brought 51:12 88:22 91:22 119:4	captured 96:24 98:17	challenge 58:19 115:3 118:3 120:6	check 5:8 6:1 48:16 56:2	citizens 47:9
bucket 16:23	captures 95:5 97:13	challenged 52:11	chief 74:4	
budget 26:14,16,18 26:23 27:4,11 87:2,20 88:15,16 88:17,24 89:4,9 89:12,16,17,22 90:3,19 94:11,21	care 64:5 66:11 70:9		child 1:24,25 2:8,15 2:16,17,21 8:1,1,4 8:4,6,19 9:10,24 9:25 10:2,4,6,8,10 10:15,16,25 11:11 12:5,7,12 13:21 13:24 14:20 15:11 15:20 18:3,4,21 18:23 20:18,22 21:11,13 22:14,16 22:25 24:9,11,11 26:5,7 27:3,19 28:3,5 30:9,9 35:8 39:11 42:10 45:23 46:3,4,8 58:24 60:18,20 63:19,24 64:4,23 65:10,16 65:18,24 66:1,2,4 66:4,18,24 67:4 67:17 70:7,10 71:7 75:4 79:7 80:15 81:23 82:1 82:12,25 84:22 85:16 86:12,24	
budget-related 90:21	carefully 117:11		charge 103:18,19 103:20,23	
budgetary-type 94:7	CAREY 71:23 72:2 72:3 120:9,24		Charles 72:1,5 120:24	
budgets 26:10 64:17,21	Carr 73:4,8		chat 5:21,23 9:25 21:2 36:2,8,8 113:25	
bug 20:9	carried 96:4		check 5:8 6:1 48:16 56:2	
built 29:21 64:8 68:1	carry 20:6 24:14 66:6		chief 74:4	
bullet 79:22	carrying 10:19		child 1:24,25 2:8,15 2:16,17,21 8:1,1,4 8:4,6,19 9:10,24 9:25 10:2,4,6,8,10 10:15,16,25 11:11 12:5,7,12 13:21 13:24 14:20 15:11 15:20 18:3,4,21 18:23 20:18,22 21:11,13 22:14,16 22:25 24:9,11,11 26:5,7 27:3,19 28:3,5 30:9,9 35:8 39:11 42:10 45:23 46:3,4,8 58:24 60:18,20 63:19,24 64:4,23 65:10,16 65:18,24 66:1,2,4 66:4,18,24 67:4 67:17 70:7,10 71:7 75:4 79:7 80:15 81:23 82:1 82:12,25 84:22 85:16 86:12,24	
bunch 36:13	case 55:8 62:20 63:15 70:13 83:3 84:6 97:4		chat 5:21,23 9:25 21:2 36:2,8,8 113:25	
bundle 1:15 50:22 59:17 97:9 104:7 113:2	cases 2:7,11,17,17 11:8,8 30:10 31:15 47:21 55:1 58:19 93:5 113:18		check 5:8 6:1 48:16 56:2	
	Cash 4:9		Charles 72:1,5 120:24	

clarification 70:17 clarify 14:19 47:4 48:8 70:20 85:5 105:6 classified 84:2 115:14 classify 114:22 clean 80:3 clear 10:18 21:7 29:13 31:14 50:6 60:20 80:21 85:19 107:13 114:24 115:6 116:18 117:12 clearing 15:17 clearly 86:25 115:10 116:11,15 client 76:3 close 82:12,15 closed 71:20 77:18 120:22 closely 29:19 closure 72:14 clothes 101:25 cloud 4:12 31:11 45:12 46:16,17,18 46:20,24 47:6 75:12,19 103:3,6 105:4,8,10,11,13 105:19 106:23 107:2,6,6 cloud-based 6:7 106:17 cobalt 13:10,11 codes 68:15 coding 76:25 coins 36:14 collaborates 118:24 collaboration 92:2 106:16 119:3,7 collect 112:13 collected 96:6 collection 80:1 collective 118:21	College 99:22 colour 101:6 column 50:1 54:20 57:8 58:5 columns 52:8,16,19 combat 79:7 combating 89:18 come 8:6,22 29:17 29:22 33:5 45:9 46:22,24 55:9,17 55:18 56:24 63:9 71:13 75:1 80:18 83:4 99:6 104:19 112:1,22 115:9 comes 24:22 64:4 96:1 111:23 119:14 comfortable 34:8 coming 45:4,10 55:6,7 58:12 71:8 81:10 85:14 97:5 97:6 comity 45:11 46:18 46:19 comment 69:13 committed 92:23 Committee 59:21 common 116:5 commonly 20:22 75:5 77:4 78:3 82:3 92:15 communicate 4:22 5:17 37:9 communication 5:14 14:12 17:6 17:13 35:17 36:20 37:15 62:2 69:21 communications 4:25 14:16 23:6,7 23:11 38:23 40:25 41:1,2 48:24 49:13 68:21,22,23 68:24 69:17,24 70:1,4 communities 13:9	13:19 community 14:3,10 companies 14:3 39:8 64:13 91:24 103:11 106:11,13 106:21,24 107:4 110:3 company 1:23 12:16 13:5 16:22 17:4,11,14,15 45:2 46:22 64:12 65:4 90:2 105:23 113:18 company's 106:19 compare 16:10 100:24 102:5 106:21 comparing 16:20 16:22 17:10,12 101:9 compensation 70:8 compete 76:11,14 complaint 23:3 complaints 23:2 complexity 47:19 compliance 20:4 comply 9:7 component 17:16 computer 32:4,5,6 60:23 76:9,12 86:21 computers 3:22 76:10 concentrating 73:13 concern 12:4 16:19 21:6 36:25 38:3 39:21 concerned 15:1 74:14 95:12 98:10 concerning 2:20 concerns 42:7,9 73:2 conclude 82:11 conclusion 83:11	92:10 101:1 conditions 22:19 conduct 9:13 10:7 13:1 21:7 63:7 conducted 59:5,5 95:3 conducting 29:25 59:6 conducts 16:16 21:9 23:18 63:21 conferences 59:2 confident 22:21 confirm 5:11 6:2 10:9 22:24 Congo 13:9 congregate 36:7 connect 5:1 connected 32:9 conscious 33:18 conservative 27:21 27:24 consider 38:19 108:12 considered 108:12 consistent 16:11 constant 109:13 110:17,19 constantly 39:2 119:12 constraining 90:19 90:20 consultation 68:8 consumer 3:9 66:15 111:23 contact 8:6 10:6,16 15:21,22 contacts 41:14 52:6 contain 82:12 contained 53:1 containing 102:10 content 9:20,21 14:11 16:24 17:7 22:10 23:8 31:13 31:17 32:3 52:5 52:12 54:20 55:4	56:11,15 57:16 64:14 73:6 76:19 77:9,13 78:8,9,12 78:14 80:22 81:5 81:16,16 82:1 83:18,20,23 84:13 84:22 85:16,25 88:10 97:23 104:15,17,19 119:23 contents 20:3 37:25 context 10:11 15:12 20:23 continually 102:22 contractors 27:25 contribute 102:21 contributes 102:18 contribution 65:9 100:6 control 18:14 24:2 24:14 69:3 70:23 controlled 43:22 44:3 controller 80:9,9 controls 18:9,13,14 18:17 19:22 21:3 21:20,22 22:1,3 23:22,24,25 24:5 24:6,17,25 25:7 25:11,23,24 26:1 62:4 69:2 70:21 70:23 71:9 convenient 47:25 120:9 conversation 37:13 85:9 90:18 91:13 99:16 conversations 37:22 69:12,21 92:14 cool 111:5 core 17:13,14 Cork 7:6 43:6,10 43:23 corporate 65:18
---	--	--	---	---

72:7,13,21 corporation 73:21 correct 2:2,4,5,19 2:21,22,25 3:5 4:16,17,24 7:14 7:17 10:17,22 28:17,18 34:6 37:19,22 43:21 44:4 51:2 53:25 54:1 72:9 75:24 78:2,5 79:21 86:1 86:9 87:21 88:1 88:16 92:16 103:17 111:18 costs 106:14 counsel 8:5,17 10:6 10:16 11:11 21:11 27:3,5 118:23 counting 102:16 countries 56:18 57:13 79:20 84:10 112:9 country 73:7 112:17,18,19 couple 92:25 course 4:18 16:22 17:11 30:21 31:25 36:19 70:18 court 71:20 83:17 120:22 cover 87:25 103:24 covering 50:21 105:4,4 covers 59:8 crawls 119:22,23 create 100:10 created 4:4 14:4 19:5 67:15 98:6 Crime 59:20 87:23 89:15 90:1,23 crimes 58:25 79:23 79:25 80:1,17 86:25 87:19 criminal 2:5 80:11 88:5,13	criminality 79:3 criteria 45:25 46:5 CRM 76:2 cropped 101:7 cross 50:15 CSA 26:21,24 27:12 29:8 49:22 73:11 CSAM 75:17 CSEA-related 74:11 CSEA-type 73:2 CSEAI 75:22 78:8 CSIS 58:18 cumbersome 44:24 45:6 Cupertino 7:9 43:10 curated 61:19,24 curious 110:16 current 2:23 currently 83:15 87:13 98:5 customer 31:4,8,10 31:15,16 33:3,9 34:20 40:4 41:13 41:17 42:1,3,4 49:5,6 54:23 76:2 86:10 customer's 31:7 customers 4:3,12 5:14 6:6,8,12 18:7 19:4 22:4,6 23:2 24:1 25:19,24 38:17,18 39:6,6 39:17 41:11 49:4 70:3 72:15 87:7 100:7 customers' 17:14 17:15 38:14,16 52:3,4 cyber 80:13 87:7 87:11,14 98:1,2 112:2	D	D 120:17 dad 111:5 daily 106:23 danger 45:23 84:2 dark 67:12 Dartmouth 99:21 data 17:15 19:23 29:2 30:4,4,12,13 30:16,20 31:15 32:8,23 33:14,16 34:5,6,7,10,19 35:10,22 36:23 38:16,20 39:1,3,7 41:9,13,25 42:4 42:25 43:15,16,19 44:2,12,14,17,20 44:25 45:25 46:1 46:13,23 48:12,14 49:8,9,24 52:12 52:12 53:22 54:8 54:19,20,21,22,25 55:3 56:3,10,11 56:15 57:7,17 58:4,20,21 59:9 59:11,13,15 111:24 112:12 database 102:10,13 102:22 104:21 109:3 database-type 76:4 databases 102:11 102:21 109:2 date 51:10 93:8,11 93:24 97:22 103:14 dated 50:20 106:5 109:9 dates 33:24 day 1:4 116:25 120:6 days 17:2 DC 3:2 DCU 79:24 88:3 deal 73:11 79:4	80:19 87:9 92:7 94:5,6 104:19 110:5 115:16 dealing 73:2 107:20 deals 72:15 105:7 dealt 86:3 debatable 115:4 debate 114:20 December 2:23 109:9,10,14 decided 99:24 deciding 95:11 decision 33:18 51:12 103:23 112:24 decisions 18:10,11 decline 5:22 dedicate 13:24 64:22 dedicated 12:7 18:5 18:8,12 26:23 28:1,4 40:2 85:3 91:17 96:25 deem 85:21 define 45:22 definitely 84:9 110:12 definitively 51:21 degree 73:3 deletion 29:3 deliberately 87:15 117:15 delivering 116:5 delivery 106:17 Dell 76:12 demand 39:18 demonstrated 58:18 Department 45:5 departments 86:14 depend 102:6 depending 10:11 32:23 33:9 41:12 41:16 47:18 61:17 87:13 101:21	depends 15:12 16:20 22:13 31:4 33:2 34:7,19 35:10 37:23 40:18 41:10,25 69:10 115:14 depicted 96:14 deploy 103:9 deployed 105:18 107:2,2 descend 82:5 describe 3:7 7:11 7:18 15:7 49:17 described 45:6 63:11 description 59:25 descriptions 50:2 design 3:18 40:11 64:17 89:17 designed 40:9,12 70:21 87:15 103:22 119:19 designing 3:8 despite 48:13 destination 119:10 detail 2:10 4:14 17:20 18:18 25:11 42:12 69:12 82:6 112:8 details 52:2 54:9,23 69:11 106:8 detect 97:12,19 detected 115:12 detection 97:23 110:21,23 determination 114:25 determinations 62:25 determine 60:19 65:1 84:22 85:24 101:23 102:1 105:23 116:23 determined 108:7 119:11
---	--	----------	--	---	---

determining 54:4 85:16	36:1,13 39:16 59:1,14 75:2,5 76:10,10,11 78:24 83:5,6 84:10 88:12 91:10 101:22 116:21	92:6	dual 81:14,18 82:6 83:12 117:16	either 5:18 42:7 74:10 77:22 80:9 89:5 110:23 117:20,23 119:7
develop 64:17 94:24 95:20 98:5	differentiation 68:20	discussion 85:10,20 discussions 57:3 68:18	due 106:14 107:5	elaborate 40:7
developed 19:14 60:14 92:12 99:12	differently 68:24 101:7	displayed 1:19	duplicates 97:19	elapse 93:21
developer 19:17,19 21:15 62:24	difficult 26:9,13 27:20 36:10 60:19 98:20 111:25 116:23	disseminate 74:10	duplicative 97:23	electronic 15:16 38:21
developer's 21:16	difficulty 83:21 88:4	disservice 63:20	duty 70:9	electronics 3:9
developers 4:4,5 19:5	digital 41:8 79:23 79:24 80:1,17 86:25 87:19,23	distinction 33:8,10 48:22 49:2 68:22 69:17	dynamic 27:14	element 75:12 90:12
developing 18:9,13 67:7 86:19 98:22	direct 55:20	document 51:2,15 51:20 96:1,2 97:10	Dynamics 75:8,25	elements 75:21 87:9
development 80:18 86:17 88:23,25 89:2,24 90:15 92:4 97:11,21,23 99:5,13,20 104:1	direction 95:18 116:3,21	documents 1:18,19 38:23 41:14	<hr/> E <hr/>	email 5:19,20 6:10 6:13 37:8 42:4 52:5 75:21,22,23
device 3:22 4:10 18:15 24:2,3,12 24:21 31:7,9,11 31:13,13,17,21 32:5,12,12,13 33:16,22 48:20 49:6,7 50:2,8,9 52:5 54:11 59:16	directions 92:5,21	doing 60:5 64:3,13 77:15 85:17 90:8 108:17 117:5	E 120:17	emergencies 45:22
device-dependent 24:22	directly 45:2,10,18 46:1,22 55:18 56:4 74:18	dollars 67:23 87:20 89:23	earlier 6:4 55:4 58:17 64:24 69:19 71:13	emergency 45:22 47:22 50:13 55:25 57:22,24 58:2
devices 3:19,20 5:16 6:17 11:22 12:15,16,17 13:12 18:16 24:6 31:9 32:2,9 33:13,14 34:5 38:21 50:10 59:14,14 69:4 71:5,7,10 76:7,8	director 1:24 8:14 8:15,16 72:7 74:2	domain 47:3	earn 88:8	employ 6:24 7:21 8:4,11 17:7 86:13
devil 69:11	disaggregate 87:8	domains 6:11	easier 47:7 95:25	employed 80:24
devote 90:7	disaggregated 74:22	domestic 2:15	easiest 1:20	employee 27:25 65:12 73:20
devoting 118:2	disaggregating 88:4	donates 89:6	easily 17:3 106:9	employee's 12:10
diagram 104:8	discover 78:6 117:9 119:24	donations 65:12,13 65:15 66:19,22,24 66:25 67:5	East 97:5	employee-driven 65:11
dialogue 29:20	discrepancy 57:11	double 81:11	easy 106:11	employees 7:4,15 8:8,12 11:9 12:1 15:1 18:21 25:18 25:21 73:16,24,25
difference 47:5 56:14 58:10 60:2 112:18	discuss 3:3,4 18:18 23:23 30:11 31:19 43:13 53:19	doubt 84:13 119:1	economic 43:20	employs 7:4 9:2 86:21
different 10:11	discusses 32:1 57:24	download 19:4 24:9	ecosystem 32:1,2 59:13 65:19	empowering 18:10 69:2
	discussing 12:24	downloaded 60:9 73:11	educating 25:6	enable 4:22 6:13 24:1 46:20 97:25 105:17
		downloads 41:14 97:1	education 13:14 25:16,25 66:2,13	enabled 32:6 38:25 73:10
		draft 63:25	educational 25:13	enables 4:7 5:13 103:11
		draw 109:23	educators 66:14	enabling 24:14
		drill 18:25	EEA 43:19	
		driving 64:14 92:23	effect 107:19	
		drop 16:23	effective 60:13 61:18 62:8 91:4 97:18 119:8	
			effectively 75:23 76:3 77:20 85:10 85:24 88:5 100:22 105:22 116:5 117:2 119:13	
			effectiveness 61:7	
			effects 13:6	
			efficiency 107:5	
			effort 100:9	
			efforts 25:7	
			egregious 84:8,12	

98:6 encounter 75:17 encountered 75:5 78:3 92:15 encourage 25:14 63:7 70:22 encouraging 25:6 encrypted 14:16 17:12 23:7 31:15 35:12,12 37:18 40:10,10 41:18 48:9,16,21,25 58:19 59:16 70:2 98:3 encryption 17:18 30:2 38:7,17,19 39:2,8,13,19 40:21 48:13 end-to-end 14:17 35:12 37:17 48:25 endangered 46:5 enforcement 7:22 8:11 11:6 15:19 15:22 22:6,7 28:21,23 29:1,7 29:10,11,19,21,25 30:2,5,7,8,13,14 30:18,24 31:23 32:7,12,17,24 33:20 34:6 35:6,9 35:11,20 36:23,24 36:25 37:20,21 38:1,3 41:22 42:6 42:14,19,21,24 43:14 44:7,19,25 45:8,8,14,24 46:1 46:4 47:7,11 48:13,16,20 49:1 49:19 53:5,13 54:10 58:14,23 59:3,4 63:5 67:16 82:10 91:5,10,16 103:16 104:25 112:4 enforcement's	58:18 enforcement-foc... 59:2 engage 13:14 36:11 86:5,6 engaged 13:16 engagement 36:24 93:20 engine 77:25 78:11 108:24 113:5,20 114:14 117:1,3 119:22 engine's 113:19 engineer 3:15 49:10 60:22 engineering 74:14 74:15,19 88:21 89:1 91:20,23 104:2 106:15,18 118:2 engineers 67:19 80:1 85:3 86:3,11 92:22 94:18 enhance 68:3 enhanced 21:22 59:24 62:3 enhancing 24:13 enormous 23:14 ensure 9:23 13:16 20:3 21:21 63:3 63:25 64:2 82:7,8 83:8 100:5,6 109:5 115:12 ensuring 9:3,7 18:6 64:5 65:24,25 70:4 entire 104:4 entirely 14:19 21:15 entirety 23:14 entity 44:3 equally 75:20 76:23 80:15 100:4 error 83:4 essential 13:11	essentially 11:3 37:9 60:23 92:10 98:9 107:10 establish 10:7 established 3:4 73:16 estimate 19:11 26:20 79:14 euphemisms 20:23 European 43:20 72:22 event 83:13 115:6 eventually 93:9 evidence 9:24 11:24 22:14 31:1 37:17 48:9 59:19 63:10 70:6 71:24 73:12 75:2 77:3 78:10,25 94:11 evidently 62:19 evolved 103:24 exactly 6:19 32:21 43:8 95:6 112:8 Examination 1:10 72:2 120:21,24 examine 86:11 examining 95:4 example 4:23 5:16 8:22,24 9:2 12:12 13:20 17:1,23 18:8,25 20:17,19 23:5 30:23 31:12 32:4 34:12,13,19 35:7,16 38:2,10 39:23 41:11 48:24 57:12 62:1,5 66:1 66:9 67:3,5 74:17 77:14 81:20 82:18 86:15 88:4 90:11 90:23 91:18 94:19 111:11 113:24 114:24 115:25 116:10,11 117:19 examples 14:23 17:25 18:2	Excel 75:11 exception 39:10,11 39:13,13 40:20,24 excess 89:22 exchange 5:23 exchanges 6:13 exciting 92:4,21 99:19 exclamation 119:15 Excuse 28:25 exigencies 45:21 exigency 46:2,3,5 exigent 45:17,20 46:7,12 47:22 exist 30:17 expand 76:1 88:2 expect 23:10 116:7 expectation 61:6 expectations 16:21 expected 22:12 100:9 expects 47:5 expensive 71:6 experience 11:6 60:17 62:17 73:1 107:5 expert 106:2 expertise 11:3 29:15 32:21 33:4 44:15 46:11 50:7 54:3 105:23 experts 34:9 59:12 explain 3:16 20:19 44:21 58:15 75:12 106:9 explaining 104:8 explanation 100:17 explicit 114:6 exploitation 2:8,17 8:1,2 9:10,24,25 10:2,4,8,10,25 15:12 18:24 20:23 22:14,17,25 27:19 30:9 42:11 58:24 87:24	exploited 15:14 39:14 exposé 118:10 expressed 36:25 38:3 extensive 106:14 extent 35:23 63:23 69:23 external 72:8,15 extortionate 110:15 extract 33:14,16 59:19 extremely 76:21 eyes 9:19 eyes-on 9:13 20:1
				F
				face 118:3 Facebook 4:19 107:16 facet 40:18 FaceTime 5:3,12 5:13,20,25 35:5,7 35:11,16,17 36:1 36:17,17,22 37:1 40:10 49:12 70:20 70:24 71:2 facial 67:8,10 101:18 facilitate 14:14 25:23 79:2 facilitated 49:22 facility 86:16,23 98:3 fact 11:25 14:11 29:23 51:24 65:21 73:8 82:1 93:9 117:20 factor 90:20 factors 90:20 102:7 factory 66:4 failed 70:9 fair 6:20 15:3 19:11 19:12 27:12 64:11 fairly 16:1

fall 10:15,21 11:9 77:1	financial 38:23 50:13 94:8,13	folk 47:23	front 1:15 57:9	getting 91:25 93:1 99:25
fallen 50:18	financially 89:20	folks 5:1 7:22 11:4 13:3 14:13 36:2 36:13	full 1:13 52:21 54:14 57:6 72:3	gift 94:17
falls 14:25	find 1:16,17 5:1 15:13 21:5 22:10 22:16,17 38:25 62:2 78:6 82:24 88:11 111:14 117:8	follow 74:23 88:14 112:4	fully 68:17	girls 96:17 114:2
false 61:3	finding 111:8,9 119:12	followed 44:14	function 3:22,23 24:15 73:3 120:2	GitHub 76:24
familiar 3:12 25:22 29:14 36:12 60:13 119:1	findings 95:19 96:9 96:10,13 114:17 117:21	following 64:2,3 113:9	functions 3:24,25 72:21 74:20	give 2:10 8:21 12:6 12:12 13:20 14:22 14:22 17:25 20:17 26:20 27:15 29:9 29:11 31:2,3 32:16 51:10 53:4 80:23 82:9 86:12 87:22 88:4 92:17 94:1 116:10
family 66:2 113:21 114:15	finds 8:20 10:14 15:24 21:10 113:6 120:1	fool 119:13	fund 89:8,10 95:3 95:11	given 14:15 16:13 17:23 26:16,25 27:6 33:20 37:21 38:9 49:9 59:1,19 63:18 65:19,20 69:19 94:11 103:20 110:6,13 118:23
far 60:17,25 61:23 74:14 98:10 103:7 115:23	finish 80:20	force 46:24	fundamental 38:11 38:17 39:5,22	gives 21:6 38:12 114:24
faster 103:7	firm 82:9,9 109:24	foreign 44:18 46:20 56:24	fundamentally 39:1 118:1	giving 58:4 65:14 65:18 78:10
favour 69:9	first 3:9,11,15 19:2 25:17 50:1,21,25 51:16 52:18 53:6 54:21 58:25 59:22 60:3,8 64:19 65:11 79:17,22 114:13	forensic 59:12	funded 96:4	glasses 101:15,17 101:22 102:2
feature 20:11 32:6 114:8	first-generation 60:15	forensics 31:25	funding 67:2,14 94:25	global 1:25 7:21 8:15,16 74:4,5 87:14 111:16
featured 96:17	firstly 23:24 72:6 75:6 114:17	former 2:5 7:21 8:11,11 11:5	further 12:20 13:4 27:15 33:5 93:7 94:24 95:14 104:3	globally 73:23 79:15,16,17 88:16
features 31:4 37:23 40:14,16 41:10 64:8	fits 110:16	forms 17:6 75:19	gain 119:19 120:7	go 6:1 9:19 20:2 23:16 33:4 34:9 36:7,17 44:19 46:14,23 47:8 48:7 54:12,19 55:4 56:2,6 57:19 59:11 78:25 82:3 82:7 85:12 87:12 92:5 98:11 99:9 102:25 112:7,7 115:22
federal 2:14	fix 20:10	forth 26:23 33:9 42:24 50:3 69:22 75:11	game 76:20 77:14 77:15,19,22 110:8 111:3	goes 19:25 20:15
feel 1:16 34:8 90:14	flag 92:14	forums 91:7 96:25	gamer 77:13,14 111:2	
feeling 93:1 100:3	flagged 81:21	forward 92:23	gamers 76:20,21	
fees 89:13	flexible 87:16	found 23:8 66:1 82:19 113:18 114:11 116:1	games 78:20	
fell 22:11	fluctuate 47:18	Foundation 94:20	gaming 76:14 77:12 111:4,6	
felt 68:3 95:18 106:1	focus 8:18 18:3 19:14 29:5 77:3 86:16 87:13 99:4 116:17	four 11:12 53:4 84:6,6	gated 62:5	
field 34:10 65:9 90:5	focused 91:14 99:18 117:23	fraction 13:23	geared 14:13 59:12 81:5	
fight 86:24 105:25 108:9 110:8 112:20	focuses 79:11	frame 15:24 47:10 47:13 101:8,9	general 8:17 9:11 14:21 52:22	
figure 27:15,16 28:7 30:18 36:5 52:13,17,19 56:9 56:13 57:8,10,13 58:4,6 79:13 84:16 109:13 111:16,17,21	focusing 117:12	framework 68:13	generally 8:2 17:23 26:8 28:2 52:2 55:4 56:21 69:9	
figures 111:20		frankly 47:7	generate 50:7	
files 77:23		fraud 8:2 26:22	generation 89:3	
filtering 60:12		free 1:17 19:5 103:20 105:2,3 107:22	geographically 43:9	
finally 83:18 107:20		freeform 62:1	Germany 7:10	
		frequently 20:12		
		fresh 116:2		

25:10 42:20 44:25 56:22 81:23 98:7 102:9 115:16 going 12:20 13:5 17:11 23:2 45:14 54:17 55:21 73:8 75:25 80:18 82:5 91:13 92:18 99:6 104:19 108:4 118:21 good 1:4,7,11,12 18:10,11 38:6 86:15 90:16 91:9 91:18 94:19 100:1 107:19 115:7,13 117:18 118:14 Google 107:16 governed 44:4 government 46:21 49:18 56:25 57:22 80:10,11 86:4,6 government's 68:7 governments 39:15 governs 74:17 grant 40:20 granted 61:13 granular 112:8 granularity 19:13 grapple 38:6 grave 63:19 great 25:11 64:5 73:4 101:2 greater 110:6 greatly 68:3 grey 117:24 grid 83:24 84:7 114:21 115:5 groom 14:8 grooming 77:7 78:16,19 92:15 93:15 group 74:9 groups 21:2 36:7 63:25 65:5 grows 102:22	guarantee 39:17 guess 85:7 guideline 23:1 guidelines 19:19,20 20:4 63:4 <hr/> H <hr/> Hackathon 91:18 91:19,21 92:8 93:18 94:5 hackers 39:3,15 hair 101:25 half 50:21 52:18 halfway 59:22 hamper 30:2 handle 11:8 27:1,2 36:5 handles 7:23 happen 14:7 20:7,9 20:10 23:6,7 34:17 51:4 93:20 happened 77:23 92:18 115:23 happening 98:25 happens 19:18 21:5 31:2,20 83:25 happy 3:17 29:17 33:4 48:1 69:11 hard 6:18 26:25 34:20 69:13 81:8 hardware 27:22 28:8,18 64:9 71:3 76:7,11 harm 68:7 69:6 75:4 78:3,25 80:3 89:19 harms 66:8,9 69:5 harness 88:20 harnessed 86:24 harrowing 82:4 harvested 96:21 hash 97:17 102:11 102:21 104:13,14 104:21 105:18 106:6,11 107:1	108:25 hashed 102:9,21 115:10 hashes 98:6 100:15 102:10 104:15,21 106:13 hashing 97:12,24 108:21 head 108:1 headcount 63:13 headed 97:11 headline 113:4 Headquarters 73:17 heard 14:2 70:6 79:19 92:8 93:20 100:15 hearing 1:5,7 11:24 62:16 73:8 120:13 held 29:2,4,6 41:9 88:16 help 3:13 4:1 6:14 8:9 11:9 15:23 16:3 18:11 19:6 21:24 24:25 26:16 28:7 33:17,24 38:12 40:5 43:16 44:13 45:13 46:10 46:16 47:5 48:17 48:22 50:1,3 51:6 52:22 53:11 54:2 54:3 57:2 58:9 77:6 80:6 88:2 91:6 93:3 94:15 94:18,21 97:14 107:18 112:20 118:17 helped 11:20,21 95:2,20 helpful 34:22 35:10 42:16 43:1 51:9 53:2 57:14 95:15 helping 85:14 helps 6:25 58:15 79:24 93:14	high 49:17 61:21 106:14 107:1 higher 61:23 highlight 96:10 highly 61:25 history 117:3 hold 31:18 40:11 54:8 118:19 holistic 12:5 13:21 18:3 26:8 65:19 home 59:20 91:24 96:15 honest 108:2 honesty 92:2 hope 47:7 97:14 hoped 93:8 host 119:23,23 hosting 21:19 hours 17:2 27:25 house 15:17 63:23 HP 76:12 Hugh 72:1,5 120:24 human 38:11 human-moderated 120:2 hundred 16:16 hundreds 84:20 <hr/> I <hr/> iCloud 4:11,13 6:4 6:5,6,9,10 24:4 31:19,20 34:4 37:8,8 41:5,6,7,9 41:11,12,16,18,20 41:23 42:7 48:9 48:12,14 50:11 51:23 52:3,4 icloud.com 6:11 ICS 2:3 3:3 7:7 8:18 10:18,23 11:10,14 15:2 16:3,15 26:16,21 63:11 idea 6:21 43:11	49:6 50:17 54:15 54:24 56:14 57:11 58:9 73:23 86:13 92:20 93:14 102:15,20 ideas 89:24 92:5 identical 102:5 104:12 identified 20:9 66:9 98:4 identifier 5:3,17,18 50:13 53:1 identifiers 37:7 identify 12:25 19:4 21:1 60:15 67:10 67:16 68:4 69:7 93:15 101:5,11 103:22 104:4,15 107:18 108:22 111:25 112:2 116:15 identifying 102:24 identity 26:22 IDs 50:12 51:23 illegal 9:11 77:10 83:21 84:3,11,13 85:22,25 113:18 113:20 114:2,5,14 119:5 illicit 36:14 iMacs 3:22 image 16:25 17:4 60:2 81:12,19,20 81:23 82:18,25 83:9 84:3 97:17 100:17,21,22 101:2,6,7,8,9,15 102:3,9 105:18 106:11,21,25 107:1 111:7,7 imagery 75:23 77:5 77:10 78:4,17 96:14,16,17,18,21 96:23,25 108:18 109:5 114:2
---	--	--	--	---

115:10 images 14:8 15:15 41:20 60:12,15,18 78:15 96:5,8 97:20 101:5,11,12 101:12 102:5,21 102:24 103:22,24 105:5 106:22 108:13,19 109:22 109:24 110:25 111:9,10,13 113:14,18,20 114:5,14,21 115:5 115:14 117:17,17 117:17 119:5,12 images' 114:7 imagine 14:1 16:25 36:10 51:22 53:15 55:2 60:24 61:1 71:8 85:12 iMessage 4:23 5:2 5:5 37:3,4,5,14,17 37:22 38:4 40:9 48:24 49:12 69:22 70:19,24 71:1 iMessages 37:25 38:2 immediate 16:1 immediately 117:7 impact 12:18 65:20 96:11 108:12 impacts 79:11 impediment 30:5 imperative 18:12 64:22 implement 64:10 65:2 implementation 74:12,16 97:11 implemented 37:24 61:17 implications 44:6 61:7 importance 69:2 important 62:7	65:2 79:1 104:16 118:20 impose 83:5 imposed 83:1 impossible 79:13 impression 12:6 63:18 improve 89:2 91:11 91:13,15 93:7 104:20 improvements 118:22 improving 88:18 in-app 62:4 in-house 106:18 inaccurate 53:1 66:10,16 inappropriate 21:19 22:4 85:21 incidences 110:10 incidents 81:2 109:25 include 18:14 22:22 23:19,19 75:7,11 109:2 includes 75:20 including 4:2 7:25 59:10 76:18,24 85:4 91:10 97:12 101:11 107:16 108:18 117:1 incomplete 63:2 increase 109:15,21 110:1 increased 109:25 incredibly 12:8 13:19 22:8 27:24 64:4 98:19,20 118:20 incremental 118:21 incurring 106:14 indecent 78:4 81:19 108:13,18 independent 68:15 indication 80:23	indicative 10:8,10 individual 49:13 individuals 37:6 79:10 110:4 industry 19:21 46:12 59:24 60:5 61:12 64:16 70:8 70:9 82:3 89:21 91:16 97:22,24 98:5 106:12,20 industry-wide 83:24 Inevitably 91:11 infected 88:6 information 25:3 27:18 29:4,6 30:3 35:19 46:21 47:9 50:10 54:23 63:1 66:10,13,16 69:6 77:18 78:6,8 84:18,19 112:22 informed 66:15 infrastructure 103:10 INHOPE 118:25 initial 9:15 initially 9:4 initiates 10:20 initiatives 25:13,16 25:25 27:23 28:2 28:5 66:7 innovation 86:23 input 5:19 INQ004187_001 113:2 inquiry 1:13 2:10 5:10 6:14 15:1 26:4 27:15 68:8 70:6 72:3 77:2 117:21 insofar 68:10 install 24:17 103:4 instance 3:20 49:12 98:20 instances 22:16	52:4 87:16 instantaneous 103:8 institutions 89:5 insufficiency 53:7 53:14 intake 47:24 integrate 106:13 107:6 integrated 71:3 integrating 74:19 integration 94:18 intended 31:8 32:2 36:6 98:11 intensive 62:21 intent 79:3 116:12 116:12,15,18,24 117:13,14,16 interact 14:5 interaction 28:20 91:4 intercept 38:2 interested 91:3 interests 14:7,7 39:22,23 internally 106:14 international 43:23 59:3 internet 78:7 80:3 87:6 94:20 108:10 117:9 119:21,24 119:25 interventions 95:15 introduce 96:3 introduced 93:10 93:25 introduction 119:14 investigate 7:24 8:2 8:3 13:6 22:8 investigating 15:4 58:19 80:4 95:14 investigation 10:20 13:8 23:17 35:11 43:2 63:8 113:17	117:25 investigations 1:24 1:25 7:24 10:24 11:15 12:2 16:3 16:16 23:18,19 27:2,12 30:1 58:22 63:22,22 investigators 16:2 investments 90:16 invitation 35:18 invitations 35:16 36:22 invite 35:17 36:8 36:16 95:22 involve 14:3 28:3 88:9 involved 10:23 11:15,16 25:13 79:5 85:8 93:18 99:13,25 involves 20:1 30:15 41:7 45:7 iOS 3:21 33:9,13,14 33:15,15,25 34:3 34:22 48:20 52:5 IP 8:3 32:25 42:5 54:22 iPad 24:18 iPads 3:12,21 iPhone 24:18 29:8 29:9 30:24,25 31:1 32:16 IPhones 3:12,20 33:8 Ireland 43:20 Irish 43:22 44:3,4,7 issue 14:20,22 17:19,22 23:16 27:6 84:24 99:18 issued 68:15 issues 7:24 8:6 26:21 27:7 72:19 95:16 iTunes 34:16 52:3 IWF 95:1,3 96:4
--	---	---	---	--

98:4,14 102:12,14 102:18 105:16,17 105:22 106:2,5,10 106:16 107:1,6,11 107:16,18 108:25 118:5,17,24 IWF000010_004 95:24	90:12 91:7 94:14 94:16,17,25 95:6 108:8 110:7,24 114:24 118:7,16 118:19,22 119:11 120:3 kinds 28:23 41:9 72:19 91:10 kitemark 61:13 kitemarking 61:18 61:18 62:7 know 5:2,3,14 6:23 7:3,5 13:11 14:1 14:13 17:16 19:8 20:22,24 25:2,3,4 33:23 34:11 35:2 36:4,6,9 37:6,7 42:10,11 43:5,6,7 43:9,18,23,24 44:6,9 45:3,16 48:15 49:21,24 50:19 51:4,8,12 53:16 54:6 57:15 57:17,18 58:11,12 60:23,23 61:1 63:7 65:15 81:3 82:14 84:10,16 85:12 86:21 87:11 88:5 90:6,12 91:3 91:12 95:15 100:7 100:8,10 102:18 107:15 108:8 110:6,25 111:1,4 111:5,6,22,25 112:16,23 113:6 114:20,24 115:21 116:17 117:10,15 117:16,18 118:10 118:16,17,20 120:2,6 knowing 26:20 knowledge 35:23 35:25 37:2,2 38:5 42:9 55:1 58:20 105:22	known 2:3 55:13 60:12 102:24 104:5,15,17 115:10 Krishnan 1:6,7,10 1:11 47:25 48:3,7 70:12,18 71:11,16 120:21	104:25 112:4 laws 83:22 lawyers 7:21 79:19 80:2 layman's 72:10 93:3 lead 1:25 7:8 leadership 72:12 72:23 leakage 69:20 learned 67:12 learning 60:16,21 74:11 86:17,18,19 Leaving 35:4 led 99:21 114:5 119:8 left 62:18 legal 7:20,21 53:7 53:12,14,15 72:7 72:14 79:17 let's 17:18 18:25 19:17 29:7 31:20 32:14 47:11 92:6 99:7 100:11 level 2:14 13:6 49:17 61:21 83:9 92:2 110:19 liaising 90:22 liaison 91:4 licenses 102:17 limit 84:23 limitations 23:4 limited 65:21 68:9 111:2,2,15 limits 84:11 101:14 line 109:24 lines 21:2 54:23 LinkedIn 76:24 links 34:4 120:1 list 20:21 98:6 105:18 106:6,11 107:1 108:25 lists 97:17 literacy 66:8,14 little 2:10 4:14 6:4	6:5 17:19,20 31:25 33:5 71:13 72:6 73:14,22 88:2 91:3 108:1 111:7,7,9 120:4 live 35:7,15,24 36:17 77:6,17,22 78:21 85:9,17 95:5,12 96:11 97:4,6,13 98:16 98:16,21,23 110:25 load 111:10 loan 94:17 local 2:12 15:18,22 locate 5:1 located 7:8 43:9 111:24 location 32:25 38:24 96:22 112:3 locked 29:9 31:1 33:14,16,22 locker 98:2 lockers 98:1 logistically 59:11 logs 32:25 London 7:5,10 long 72:24 longer 33:19 106:20 look 1:21 9:19 18:23 20:2 25:4 31:5 33:7 50:20 53:2 57:1 59:14 61:25 75:3,6 78:24 92:6 94:7 95:9,21,22,25 96:5 99:7 100:11 100:12 101:22,24 104:6 106:3 108:14 116:2 looked 96:2 113:6 looking 9:23 18:1 25:24 28:22 29:24 36:11 38:1 39:3
J	Jacqueline 74:5 January 113:4 118:9 119:4 job 66:3 81:1 John 73:4 join 108:8 joined 2:18 72:25 joining 36:13 journalists 118:19 journey 119:10 judge 66:16 July 59:7 jumped 94:5 Justice 45:5	L		
K	keep 53:3 65:6 84:18,19 91:12 keeping 79:6 keeps 49:24 kernel 92:20 key 20:22 49:5,5 87:1 89:15 96:10 keys 31:9,10,14 35:13 40:11 48:21 49:11,14 kids 114:1,4,15,15 115:20,25 116:13 116:22 kids' 61:19,22,24 62:1,3 113:21,21 113:25 kind 16:19 39:24 42:8 49:24 77:5 79:3 80:12,13	labour 65:24 66:1 lack 30:3 58:20 landscape 94:23 large 8:7 43:11 46:7 57:11 61:2 65:13 79:10 80:5 110:21 largely 87:4 88:19 99:15 116:4 118:4 larger 109:20 late 34:23 launched 58:22 66:12 law 7:21 8:11 11:5 15:18,22 22:6,7 28:20,23 29:1,7 29:10,11,19,21,25 30:2,5,6,8,13,14 30:18,24 31:22 32:7,12,16,24 33:20 34:6 35:6,9 35:11,19 36:23,24 36:24 37:20,21 38:1,3 41:22 42:6 42:14,19,20,24 43:13,14 44:4,6,7 44:18,19,24 45:7 45:8,14,24 46:1,4 46:11 47:7,11 48:12,15,20 49:1 49:18 53:5,13 54:9 58:14,18,23 59:2,3,4 63:5 64:2 67:16 82:9 91:5,9 91:16 103:16	6:5 17:19,20 31:25 33:5 71:13 72:6 73:14,22 88:2 91:3 108:1 111:7,7,9 120:4 live 35:7,15,24 36:17 77:6,17,22 78:21 85:9,17 95:5,12 96:11 97:4,6,13 98:16 98:16,21,23 110:25 load 111:10 loan 94:17 local 2:12 15:18,22 locate 5:1 located 7:8 43:9 111:24 location 32:25 38:24 96:22 112:3 locked 29:9 31:1 33:14,16,22 locker 98:2 lockers 98:1 logistically 59:11 logs 32:25 London 7:5,10 long 72:24 longer 33:19 106:20 look 1:21 9:19 18:23 20:2 25:4 31:5 33:7 50:20 53:2 57:1 59:14 61:25 75:3,6 78:24 92:6 94:7 95:9,21,22,25 96:5 99:7 100:11 100:12 101:22,24 104:6 106:3 108:14 116:2 looked 96:2 113:6 looking 9:23 18:1 25:24 28:22 29:24 36:11 38:1 39:3	

40:19 42:15 47:14 48:10 53:8 58:16 67:7 78:12 84:8,8 87:3 99:19 105:7 105:15 106:8 looks 14:20 39:7 69:10,12 72:13,18 117:4 120:4 lose 31:8 82:19,20 loses 49:6,7 losing 84:4 lot 80:4,13,15 87:5 111:24 lots 106:1 love 39:10 91:12 loved 38:23,24 lunch 71:12	man-hours 67:22 managed 102:11 management 76:3 mandate 12:24 manual 20:15 manually 106:24 manufacture 12:16 12:19 manufacturers 12:20 76:12 manufacturing 3:8 12:14,17 13:12 65:25 March 59:5,6 margin 102:6,7 marketing 3:8 marks 119:15 Marrus 1:9,14 120:19 mask 119:13 masking 117:15 mass 36:6 mastermind 88:6 match 65:12 104:5 104:17 matched 104:14 material 8:19,22 9:24,25 10:5,9,14 10:16,20 11:1,4,7 14:25 15:9,12,24 16:17 18:24 20:18 21:5,13,19 22:5 22:15,17,22,25 29:8 30:25 42:8 42:11 47:3 60:9 75:17 79:7 82:12 84:23 85:17 86:12 87:10 108:9,22 115:15 materials 12:21 matrix 82:2,4 matter 39:12 46:11 106:6 matters 7:25 18:21 27:4 46:8	mature 60:17,25 me.com 6:10 mean 25:15 40:8 50:4 91:18,21 94:16 100:3 101:4 102:16 105:21 107:14 109:23 112:21 115:13 meaning 53:14 57:24 106:18 means 43:24 44:18 69:22 72:17 75:12 75:13 93:3 102:22 103:6,8 105:22 measures 59:25 mechanism 74:23 83:5 112:4 mechanisms 22:4 81:22 88:8 media 12:15 13:25 14:2 16:22 17:4 17:10,16 36:15 37:12 61:5 62:2 64:13 68:21,24 69:18,20,22 medical 38:22 meet 14:4,6,8 36:16 37:12 46:5 53:15 63:4 meeting 14:14 64:1 67:18,23,25 meetings 91:6 meets 45:25 Melissa 1:9,14 36:4 120:19 member 10:14 11:24 12:3 16:15 16:18 62:15 89:5 107:6,11 118:25 members 10:23 11:14 59:4 64:16 105:17 106:20 107:16 membership 89:13 meme 17:1	mention 6:18 19:9 68:17 77:1 mentioned 6:4 12:15 13:25 18:22 19:20 20:13 22:9 26:7,22 27:2,20 28:8 38:14 40:9 46:16 55:4 58:17 61:20 62:13 64:5 64:24 69:6 76:7 95:1 merely 9:1 message 37:5,9 met 54:18 63:6 method 97:24 methods 14:11 17:13 Metropolitan 59:7 MIC000012_003 100:13 MIC000018_003 104:7 MIC000019_002 106:4 Microsoft 71:24 72:8,24,25 73:13 73:14,15,18,18,19 73:20,23 74:2,10 75:3,16 77:25 79:5,11,23 80:24 81:18 82:15,17 83:14 84:5,17 86:13,15 88:15,22 89:5,19 90:3,14 91:5 92:23 93:17 94:8 95:2,11 96:5 98:5,10,11 99:12 99:24 102:25 103:14,20 105:16 106:10,12,16 107:22 108:17,21 108:24 109:7 110:18,24 113:5 114:11 115:24 118:11,13,24	Microsoft's 80:23 97:17 110:19 113:13 middle 97:15 100:17 million 17:3 26:19 109:18,19,20 110:15,15 millions 6:20,20,21 6:21 11:23 16:14 19:10 87:20 106:22 110:14 116:25 Milward 71:24 72:1,5,6 79:9 89:15 95:25 97:8 100:14 113:3 120:24 mind 51:16 78:10 82:13 84:21 119:22 120:5 mining 13:6,10,17 13:17 misleading 56:19 missed 117:24 Missing 15:14 mistake 83:3 Mixer 76:19 77:6 77:10,20 MLAT 44:19,22,23 45:15 46:14,23 47:8,12 55:5,10 55:12,21 56:19,22 Mm-hm 28:11 53:23 mobile 3:20 mobile-only 96:24 model 64:25 moderate 14:11 64:14 85:10 moderating 16:24 moderation 14:3 14:17 81:5 85:18 moderators 17:7 80:22,24 81:1
<hr/> M <hr/>				
mac.com 6:10 MacBooks 3:23 machine 60:16,21 86:17,19 machines 88:7 macOS 3:23 mail 6:9,10 41:11 main 12:14 maintain 31:14 34:14,14 35:15 42:24 49:5,11,13 59:15 maintained 41:13 41:15 59:13 102:13 maintaining 87:6 88:17 maintains 49:5 59:9 majority 7:13,15 7:16 11:19 13:10 14:16 47:21 86:16 make-up 8:9 making 34:8 58:14 90:15,16 92:24 100:6,9 112:21				

83:18,20 84:15 85:2,5,7 moment 19:1 47:25 112:14 money 26:3 88:8 89:6 monies 27:19 monitor 80:22 monitoring 85:20 106:19 107:8 month 109:11,12 months 93:21 94:2 94:3,4 109:8 morals 64:3 morning 1:4,7,8,11 1:12 mother 70:6 motivation 95:10 move 7:7 37:13 87:16 104:2 multiple 9:17 20:14 65:5 79:20 98:17 98:24 113:18 music 4:6 41:14	79:18 81:4 82:7 102:12,14,17 109:2,8,18,22 110:7,14,20 111:22 112:2 118:24 near 58:5 necessarily 23:13 40:16 45:3 necessary 22:23 26:12 65:1,3 82:5 necklace 101:25 need 6:1,2 17:20 24:17 27:6 29:22 30:18 42:25 47:19 48:16 81:25 87:17 93:6 103:4 113:7 needed 92:3 115:8 needs 27:7 59:23 78:10 81:12 network 4:15 37:13 77:18 80:7,8 88:6 networks 4:19 67:17 80:14 88:11 never 62:22 90:5 117:1 119:16 new 2:13 28:8 31:13 74:11,17 85:13 86:11,23 89:1,24,25 92:5,5 97:11 116:3 119:12 news 66:8,11,14,15 66:17 117:20 NGOs 13:14,14 65:9 66:13,22 67:1 91:17 118:18 non-content 52:12 54:18,21,22,24 55:3 56:3,10 57:7 non-emergency 55:24 non-exigent 44:20 47:17 non-profits 66:23	North 67:16 notably 21:18 note 9:1 34:22 104:16 notes 41:15 November 21:14 91:22 NPCC 90:24 nude 113:21 114:15 number 5:19,20 7:4 10:11 27:21 27:24 30:16 37:8 50:17 52:8,9,9,10 56:17 59:1 61:2 67:22 73:24 76:17 76:23 79:5,10 81:1,2,7,9,22 84:15 89:7 91:6 97:21 100:15 102:7 104:21,22 109:15,17,20,24 110:12,18 111:13 120:5 numbers 17:11 42:5 86:13 100:23 100:24,25,25 107:1 109:21 numerous 18:2 45:7 nutshell 72:10 75:8	offences 60:2 offender 15:21 offer 4:2,5,6,9 6:6 23:25 24:5,8 25:18 31:5,7 41:7 offers 4:11 75:3,16 offhand 34:1,25 Office 2:13,14 75:7 75:10,15,20 officer 74:4,6 officers 7:22 8:12 11:6 30:8,13 offices 7:5,5 official 1:23 Oh 28:9 okay 70:17 old' 114:3 Omegle 113:25 114:1,3,4 115:20 115:21,25 116:22 once 9:5 66:4 102:9 115:21 one-on-one 68:21 90:10 OneDrive 75:18 78:13,14 81:21 82:20 ones 38:23,24 99:24 oneself 107:10 ongoing 68:9 online 14:4,25 18:4 26:24 27:11 34:13 34:14 49:22 65:21 66:9,18,24 67:4 68:7 69:5,7 74:4,5 79:6,12 85:14 97:20 107:8 113:17 online-facilitated 26:5 65:10 70:7 onwards 23:23 34:3 94:10 108:15 open 1:3 37:12 62:23 71:22 77:17	77:20 120:18,23 open-source 76:25 opening 97:3 operate 7:20 103:5 105:10 operated 115:11 operates 4:21 105:12 operating 3:19,21 26:18 33:15,19 operational 94:8 opportunities 13:16 67:1 opportunity 14:22 67:12,13 opposed 26:21 55:21 opted 31:16 option 111:6 options 31:22 32:17 order 5:17 29:21 46:22 47:8 93:5,6 103:5 108:8 orders 34:13,14 organisation 67:6 67:15,25 74:6 80:12 91:1 103:9 105:24 107:23,25 108:2,3 organisations 89:8 89:13 90:8 94:9 95:7 102:19 103:12,15 104:25 107:14 108:7 110:2,3 118:15,18 119:1 original 96:22 other's 37:7 outcome 26:12 98:10 Outlook 75:20 82:21 outside 27:5 46:10 54:2 61:4 overly 53:20,25
N				
N 120:17 name 1:13 36:4 52:3 72:3,5 111:4 111:6 named 10:1 narrative 57:20,23 narrow 8:18 87:14 nation 56:22,22 80:10,11 83:25 90:13 national 15:14 59:20 89:15 90:1 90:23 111:21 nature 14:15 26:25 49:9 63:2 65:19 NCA 60:5 89:21 90:18 91:10 NCA000354 59:18 NCMEC 15:17		obstacles 106:17 obtain 30:13 32:8 39:3,4 46:22 59:9 obtaining 32:19,20 obvious 23:10 obviously 3:23 9:10 9:20 10:25 12:14 23:1 86:10 occasionally 75:21 occurring 35:14 60:2 occurs 15:23 October 96:7 106:5		
		O		

54:5 oversee 72:21 overview 49:17	parents' 24:13 41:1 41:2,3 Parliament's 59:20 part 30:11 33:18 39:25 40:3 52:20 54:13 56:9 57:5 64:7 72:12 75:19 80:17 89:2 90:25 91:1,1 102:8 110:1 119:6 particular 18:7 19:15 26:6,24 27:12 28:18,19 30:1,23 32:15 34:19 35:24 38:3 42:15 47:14 48:10 49:22 61:14 79:6 112:19 114:21 115:1 117:4 particularly 12:19 30:15 36:20 46:18 61:5 68:4 87:9 111:23 parties 19:15 27:5 partly 77:17,17 partnership 12:25 66:12 parts 74:14 86:18 88:21 passcode 29:10 31:2 32:16 passwords 38:22 pastime 76:22 pause 10:12 44:21 75:14 pay 4:7,9,10 70:8 paying 36:14 payment 4:7 peaked 50:17 peaks 87:12 peer-to-peer 4:24 48:23 67:17 people 4:10,25 6:16 6:24 8:10 11:13 14:9 25:21 36:7,8	36:13 65:7 74:24 76:22 77:21 85:8 86:5 92:1 100:18 111:9 120:7 perceives 46:4 percentage 52:13 perfection 118:23 performs 93:5 period 96:6 periods 18:16 perpetrator 29:8,9 35:6 41:22 perpetrators 79:3 person 5:17,21,22 5:22 36:6,16 45:23 72:17 115:1 person's 5:3 personal 23:11 38:21 perspective 63:24 73:22 PhD-level 86:21 phone 5:18,20 31:22 32:3,8,10 32:15 34:5 37:7 42:4 PhotoDNA 80:18 80:19 85:4 88:18 88:23,25 89:3 90:15 95:20 97:18 99:5,7,11 100:16 100:19 101:16 102:15,20,23 103:1,5,14,16,24 104:1,3,3,8,22,24 105:4,8,10,12,17 105:19 106:12 107:20,22 108:12 110:2 115:11,15 photographs 22:15 38:21,22 41:3,4 photos 32:5,20 41:14 52:5 phrase 83:7 85:8 92:12	pictures 114:7 piece 85:16 pillar 101:24 piloted 61:14 place 13:9,10,13 21:4 60:3 61:13 62:20 65:23 66:1 78:16,17,20,22 81:11,16 85:11 88:13,22 91:22 92:9 93:15 112:3 placed 84:24 places 12:19,20 13:1 plan 1:18 platform 5:4,13,15 6:10 14:1 17:5 18:13 19:3 20:8 21:15,17,23 22:3 35:12 36:10,16 37:6 40:1,6,9 64:6 68:25 69:20 76:14 76:19,25 77:20 100:4 102:23 103:3 104:23 106:19 107:7 110:24 111:1,12 platforms 3:14,18 4:21 17:2,12 21:2 21:20,21,25 22:20 23:9 26:15 34:18 36:2 39:2 61:12 61:14 62:22 64:1 69:18 71:2 76:23 77:3 81:3,10 82:14 84:5 106:23 106:25 108:22 111:14,24 play 76:20 77:21,22 77:23 86:25 played 77:23 players 46:12 60:5 77:18 playing 77:14,14 77:19 111:3	PlayStation 76:15 please 1:8,13,16,22 8:25 15:10 20:19 33:11 40:7 49:16 50:24,25 51:15 52:15 53:3 56:6 57:19,21 58:1,6 58:15 59:17 61:9 66:6 68:11 72:4 73:14 75:2,6 76:1 79:4,8,24 94:6 95:22,23 104:6 106:3 108:14 113:1,8,10 pm 71:17,19,21 120:12 point 6:12 14:20 35:4 38:6 48:7 69:14 71:1,12 74:24 79:22 82:22 120:10 points 31:24 98:22 114:9 118:14 Police 59:7 99:17 policies 63:25 policing 90:10 policy 74:11,17 86:4 policymakers 86:5 Polinsky 1:9,14,15 36:4 70:16 120:19 poor 13:19 popular 9:17 20:13 76:22 114:1 populate 31:13 porn 113:21 114:15 116:13 pornography 2:17 9:12 22:17,18 60:18,20 67:18 113:5,13,24 116:16 portion 46:7 55:2 64:16 65:15 89:16 position 24:21 34:2
---	---	--	--	--

<p>69:23 70:1,10 positives 61:3 possession 15:15 possible 36:15,19 36:19 40:24 47:23 71:6 77:13,16 87:22 106:24 111:19,21 112:7 112:10 post 33:14,15 77:21 potential 23:15 69:6,19 96:12 potentially 38:24 78:13 79:2 81:23 83:22 85:20 90:3 92:14 97:6 99:1 110:22 119:5 powerful 71:9 PowerPoint 75:11 practical 44:18 practically 100:16 practice 25:1 47:20 68:15 83:24 105:21 pre 33:13 precedent 117:3 precise 79:13 87:19 87:23 115:2 precisely 80:25 112:23 predominantly 86:22 111:8 prefiltering 60:8 prescreening 60:8 prescriptive 9:9 presence 6:15 43:5 43:6,9 59:3 preservation 29:2 preserve 31:6 president 74:8 press 93:23 presumably 78:4 115:11 pretty 77:15 82:4 104:12 111:2,14</p>	<p>prevalence 99:16 prevent 97:18 preventing 60:2 previous 16:10 28:13,14 42:2 109:20 117:6 previously 96:3 106:13 pride 29:20 42:23 primarily 15:2 primary 11:11 prior 31:13 73:1 priorities 26:22 prioritised 30:8 priority 38:12 privacy 17:13,14 17:18 19:22 38:9 38:10,13,15 39:18 39:21 40:15 42:20 53:13 61:6,8 62:3 private 9:21 14:12 14:15 23:6,11 36:20 37:15 61:5 68:23 69:17,20,24 70:1,1,4 84:18,19 proactive 63:15 64:4 106:19 107:7 proactively 25:14 probably 11:12 26:18 76:18 89:22 98:14 problem 13:18 79:7 problems 22:5 process 9:18,22 19:16,25 20:16 21:12 23:5 37:11 42:18 44:13,19,22 44:23,24 45:2,6 45:10,15,18,18 46:14,23 47:8,24 55:5,10,12,22 56:23 59:10 62:21 68:9 81:17 83:12 83:13,15 processed 45:4</p>	<p>68:18 processes 45:1 processing 42:19 103:8 produced 114:2 product 35:23 93:22 productions 53:17 products 3:12 4:18 6:16 13:7 63:16 64:18 65:20 75:2 75:5,6,7,9,10,16 77:4 79:1,2 80:23 83:14 84:5 professional 73:1 professionals 86:4 programme 4:11 13:9 25:19 30:7 58:23 62:24 65:14 programmes 64:9 65:3,22 progress 92:24 progressive 99:20 prohibit 19:21 62:1 prohibits 9:10,11 project 66:8 88:20 projects 65:3 proliferation 66:10 77:5 prominence 38:9 promoted 2:23 prompted 99:4 114:4 116:2,20 117:10 118:1 proper 30:21 52:25 92:3 properly 115:20 proportion 65:14 87:23 proposals 68:12 proposition 90:10 prosecutor 2:5,7,12 36:12 prosecutors 8:11 11:5</p>	<p>protect 26:14 38:16 39:7,21 40:15,25 protected 39:24 protecting 12:9 40:2 100:7,8 protection 38:18 39:11 40:17,19 protections 48:13 62:6 prototype 92:12,18 93:9,25 provide 13:15,15 20:25 26:13 27:3 27:18 30:20 33:1 35:9,22 41:24 46:1,13 48:21 49:8,8 66:13 67:21 68:11 79:13 83:11 84:15 111:19,21 115:22 provided 6:11,12 20:21 29:14,15 35:19 47:20 48:20 49:4 52:12,13 54:9,20,24 56:11 56:12 57:7,17 58:13 67:13,24 94:21 103:14 105:16 107:22 113:7 provider 15:16 66:11 provides 4:1 44:8 94:9 providing 71:10 provision 54:18 56:15 58:3 provisions 45:11 46:18,20 prurient 14:7 public 1:5 9:20 11:24 12:4 16:15 16:19,24 17:1 47:3 49:4 51:2 62:15 86:4</p>	<p>public-friendly 98:9 publicity 118:12 publicly 119:25 publish 51:6 published 19:24 51:4 86:8 publishing 51:13 punctuation 119:15,18 punishment 82:21 82:25 83:6 purchase 4:4 19:4 purchased 27:22 purchases 34:15,16 34:17 62:4 purpose 28:19 40:21,22 80:2 82:6 97:1 108:6 purposes 39:16 44:18 45:3 46:3 put 13:8,13 19:18 21:4 49:16 62:22 63:4 76:6 84:7 93:17 100:5,21 115:17,20 116:25 putting 63:6 111:7</p> <hr/> <p style="text-align: center;">Q</p> <p>qualified 105:24 107:23,25 108:2 quarter 27:11 queries 78:6 116:25 118:8 query 120:4 question 10:3 11:21 16:13 20:5 30:1 32:20 33:5 40:13 48:25 62:15 65:17 69:14 70:5 100:1 105:6 118:14 questions 3:17 8:1 25:20 29:16 37:3 61:7 70:12,14,15 94:7</p>
---	---	--	---	---

quickly 15:23 98:4 98:15	112:20 115:5 117:8 119:10,16	registration 54:22	73:6 103:22 108:22	54:18,19,25 55:3 55:4,6,8,16 56:1,3 56:8,10,11,15,18 57:4,6,12,16,23 57:24 58:2,11,14
quite 11:1,25 16:15 20:12 27:13 38:8 47:7 57:11 61:18 63:10,12 71:5 118:5	reason 15:19 17:8 39:25 89:14 110:1	registrations 42:4	removed 21:14,17 21:18 62:10 98:4 106:18	require 45:19
<hr/> R <hr/>	reasonably 22:21	regulated 69:24	removes 82:16	required 15:16 62:4 75:13 82:4
R&D 64:17 89:22	reasons 6:19 23:10	regulating 69:8	Repair 25:19	requirement 5:5,25
raise 17:19 110:7	recall 34:1 97:3	regulation 69:9,25	replicate 114:19	requirements 44:7 63:6
raised 42:6,9 69:14	receive 23:1 30:10 42:10 45:24 58:25	regulations 9:8,9	replication 81:15	requires 24:3 45:8
raises 61:6	received 23:3 34:22 49:20 52:9,19 55:17 56:8 57:5 58:3	regulator 68:15	report 8:14,15 15:13 22:4 50:5,6 50:21 57:20 66:19 74:7,8,9 80:8 98:22 99:16 106:4 110:5 112:13 113:6 117:20	research 33:4 47:19 86:15 89:17 95:3,11,22 98:11 98:14
raising 12:4 16:19	receives 42:13 47:11 109:18	regulatory 68:13	reported 109:22,25 114:18	researchers 86:11 113:24
range 72:21 85:4 91:23,23 107:14 108:21	recognise 12:16 101:17	rejected 52:11,21 52:23,25 53:6 54:14 56:9 57:6	reporting 74:3 79:18 110:20	reside 12:8 37:25
rate 57:12	recognition 67:8,10 101:18	relate 27:17 46:8 54:10 65:15 76:18	reports 8:16,17 17:3 22:5,6,7 51:7 51:13 82:7 109:8 110:12,17	resolved 106:6
rates 110:21,23	recommend 61:25	related 49:22 50:10 50:11 51:22 65:23	represent 91:2	resort 83:16
rationale 100:2	record 35:18 76:20	relates 112:11	representatives 25:22	resources 12:7,23 13:15,22,24 18:5 18:9,12,20 26:12 27:25 28:4 29:13 40:1 63:13 64:22 65:3,4,6,6,8,25 84:23 87:15,19
raw 12:21	records 34:14,15 34:16 35:15 38:22	relation 16:6 86:7 88:3 94:12 95:4 108:13,18	request 5:21 29:1 30:14,15 35:20 42:13 44:20,25 45:3 47:12,18 52:24 53:1,5,6,12 53:15,20,25 54:4 55:11,21	respect 60:12,14 65:17
re-engineer 112:12	recorded 96:22 98:1	relations 72:15 91:15	requesting 45:7,25 56:22 59:11	respects 90:6
re-think 118:2,11 118:13	Redmond 74:19	relationship 24:4 76:3 91:9	requests 28:23 42:20,22 43:14 44:2 46:8 47:20 47:22,24 49:18,21 50:2,8,9,9,11,11 50:13,14,17 51:17 51:19,22,22 52:2 52:9,10,10,11,18 52:20,23 54:13,15	respond 47:22 81:6 116:17 117:4
reach 101:1	refer 1:17 4:24 15:18 51:22 85:8 113:7	relationships 13:13		responding 42:19 42:22 47:10
reactive 27:1 63:10 63:12,18,24 64:12	reference 66:19,20 97:15 113:10	relatively 63:13 110:17		responds 57:25 118:7
read 91:19 113:12	referral 81:12 111:22	relevance 34:11		response 8:19 12:3 14:24 16:18 26:5 47:13,17 54:25 56:15 57:12 58:17 60:7,10 61:16 64:15 120:3
reader 38:8	referrals 81:4,10 109:16,18 110:14	relevant 8:13 15:18 32:24 33:1 57:10 58:21		responsibilities
Reading 73:17	referring 113:25	reliance 49:7 61:1		
real 103:10	refers 50:9,11	rely 11:3		
real-use 93:4	reflect 27:25 67:22	relying 68:13		
realised 68:1 98:15	reflected 12:23	remain 22:20		
realistic 90:1,9,12 93:24	reflective 81:2	remained 109:13		
really 11:3 13:18 13:18,23 27:4,6 31:19 33:2 34:19 36:5 39:8 40:19 42:23 69:11 75:16 77:1 81:25 91:21 92:4,21 93:4 98:13 99:17,23 105:24 106:2 108:7 111:1	reflects 27:4,22 56:18 67:5	remaining 94:6		
	refuses 29:9 31:2	remains 9:5 98:19		
	regard 25:8	remember 56:13 79:1		
	regards 22:23	remind 19:1 37:4 41:5 48:17 51:18 62:9		
		remit 7:18		
		remove 22:24 23:3		

<p>7:19 64:1 responsibility 12:9 12:11,13,22 13:2 17:24 18:5 74:3 74:21 110:4 responsible 9:3,7 10:19 15:2 53:16 74:12 80:17 90:22 responsive 30:21 43:1 54:8 restrict 82:14 restriction 29:3 restrictions 9:12 61:21 62:24 70:19 result 13:8 30:6 61:3 91:25 117:19 118:4 resulted 58:3 92:3 resulting 91:20 results 21:12 109:6 113:14,19,20 114:14,20 115:6 116:6,6 117:13,22 119:4 120:1 retail 7:3 25:17,17 25:21 retailers 4:8 retain 31:9 32:25 retained 52:16 retains 31:10 return 4:13 17:18 48:2 71:15 returned 66:2 reverse-engineer 108:4 review 9:6,13,18,19 9:22,23 10:5,7,14 18:22,23,25 19:16 19:25 20:1,16 21:7,9,12 23:4,11 23:20 62:21 81:17 81:24 83:23 reviewed 20:18 83:10,11 reviewer 21:9</p>	<p>reviewers 9:2,3 20:1,2,25 22:9 reviewing 10:25 60:18 reviews 84:21 richness 104:21 right 2:1 7:11 10:18 11:16 26:11 28:17 34:24 38:11 39:5,20 40:15 48:11 64:3 75:25 77:24,25 79:20 82:22 86:2 89:11 91:25 94:13 95:2 95:4 99:6 102:8 103:13,21,25 109:17 114:23 right-most 57:8 58:5 rights 39:22,23 73:5 105:17 ring-fence 26:10 64:16 ring-fencing 64:21 64:25 rise 110:15,21 risk 15:21 63:6 risks 12:25 risky 115:2 robust 18:9 role 1:22 2:24 59:24 63:16,19 74:3 87:1 roles 2:20 rolled 30:6 33:25 34:23 room 36:13 92:1 rooms 9:25 roughly 19:6 27:11 81:2 83:24 102:16 109:13 110:17,22 row 52:15 56:5 57:1 58:2,6 rowing 62:16 run 3:21 4:15 72:12</p>	<p>103:6 running 24:23 33:13 34:3 88:6 runs 24:20</p> <hr/> <p style="text-align: center;">S</p> <hr/> <p>safe 64:6 65:7 79:6 116:24 safeguards 22:22 61:13 62:20 64:17 safer 100:10 safety 1:24 2:1,21 8:4,4 10:6,16 11:11 12:5,8 13:22,24 14:20 17:22 18:3,4,6,21 21:11 26:7 27:3 28:3,5 30:10 46:3 46:8 63:19,24 64:5,23 65:16,18 66:18,24 67:4 74:4,5 79:12 113:17 118:13 sanction 83:5 saturation 101:6 saw 98:15 saying 3:15 34:22 35:1 55:11 says 43:22 52:1 56:20 88:24 120:3 scale 6:14 11:22 16:14 86:13 101:21 117:14,24 scan 100:21 106:24 scanned 83:9 scenario 29:7,12 31:23 35:8 scientists 86:22 scope 76:5,18 77:1 78:23 scratching 108:1 screen 1:20 49:16 50:24 53:3 56:6 59:18 95:23 96:1 100:13 106:4</p>	<p>113:2 scroll 58:1,5 scrutiny 61:21 search 21:1 36:3,4 42:10 74:17 77:25 78:5,11 108:24 109:6 113:5,14,15 113:19,20,23 114:1,3,14 115:7 115:16,20 116:1,3 116:11,12,12,18 116:22,24,25 117:1,2,4,12,14 117:19 118:7,11 119:6,14,16,17,18 119:22 120:8 searched 117:2 searches 115:9 117:7,7 searching 78:4,17 114:4 116:15 second 3:10 18:18 28:25 53:19 59:12 61:9 113:7,8,10 secondly 68:14 Secretary 91:24 section 53:8 97:10 97:14 104:13 sections 104:4 secure 64:6 70:4 security 1:25 2:20 7:21,23 8:6,13,15 8:17 18:6 38:15 39:18 87:6,7,11 87:14 see 17:6,9 35:17 46:6 50:2,15 52:1 52:8,17 54:12,17 55:5 56:5 57:4,9 57:15 58:1,2 59:22 62:17 67:20 75:21 76:4 81:3,7 81:10,20 89:20 93:5 95:16 110:16 118:21</p>	<p>seek 23:3 38:16 52:2 seeking 46:21 53:22 seemingly 110:19 seen 22:14 64:13 109:15,21 119:16 Select 59:21 self-generated 108:18 self-regulation 68:14 sell 17:15 38:15 send 55:20 senior 8:15,16 72:7 72:17 74:2 sense 112:10 sent 81:13 sentence 48:18 separate 80:19 serious 96:19 seriously 13:3 serve 45:1,10 serves 8:5 service 4:12 6:13 15:16 30:21 31:6 31:7,8,16 41:7 49:3,10 52:25 66:11 75:21 82:15 103:1,18 services 3:10 4:1,2 4:6,6,9,13,21,25 5:1 6:6,16 23:25 33:2 34:20 42:1 42:13 63:16 75:3 76:17 81:3 86:10 97:20 105:8 108:23 serving 117:13 session 1:3 70:13 71:14,20,22 92:11 120:10,18,22,23 set 18:16 24:6 25:12,24 28:18 53:20 88:17 89:4</p>
--	--	---	--	---

sets 25:21	significant 60:1	3:18 18:13 20:8	55:1 66:18,22	15:7 18:1 19:9
setting 24:3 96:15	65:22 91:19	64:9 71:2 76:3,4	67:1,4 88:15,17	23:23 27:16 28:22
settings 41:16	109:21 118:6	99:13 103:5	88:24 111:19	33:7 38:8 42:16
severe 82:21	significantly 59:23	sole 80:2	specifically 14:24	43:13 48:10,18
sex 2:15 79:7	similar 14:6 37:3	solution 41:8 75:19	25:10 26:1,5	49:15 51:9 53:3
sexual 2:8 8:1,19	42:2 73:3 97:22	91:20 105:19	57:15 61:15 66:23	53:19 58:16 72:20
9:10,24,25 10:2,4	101:1,3,4,12,14	106:17,23 107:2,6	68:12 69:25 72:18	73:15 79:9 87:18
10:8,10,15,25	102:2,4 104:8	107:7	specified 52:10	94:10 108:15
15:11 18:24 20:18	114:7	solutions 6:7 94:19	speed 107:5	109:9 113:7,8
20:22 21:13 22:14	similarly 32:11	97:12,21	spend 26:11 65:5,6	States 2:15 56:20
22:16,25 26:6	57:16 112:1	someone's 81:21	80:4 95:13	56:23 67:6 83:22
27:19 30:9 42:10	simpatico 32:3	83:3,14	spending 24:12	84:3
58:24 65:10 67:11	simple 59:25	soon 47:23 93:13	spends 26:4,21	statistic 56:20
67:11 70:7 75:4	simplest 103:3	sooner 93:16	87:24	statutory 79:18
80:16 81:23 82:1	simply 25:14 32:17	sorry 7:15 12:13	spent 27:10,11,19	stay 120:7
82:12,25 84:22	100:21 104:11	20:5 25:2 28:9,9	28:7,14,18 65:4	stayed 110:22
85:16 86:12,24	single 9:14 98:16	33:23 35:2 43:25	67:3 114:19	step 42:12 85:9
87:9,24 88:3,10	106:21 116:24	45:20,21 50:19	squares 84:7	stepping 85:20
88:15 95:5,13	singular 40:21,22	53:8,9 55:11,24	stack 17:17	steps 10:11 15:7,9
97:2,13,19,25	sit 72:12,22 74:15	66:5,6 105:6	staff 7:9 47:23	15:24 24:16 25:11
99:15 104:15	86:9 118:1	sort 6:7 8:10 11:15	86:10	42:15 45:7
106:1 107:9 108:9	site's 113:23	12:1 15:8 16:17	stage 32:17 68:10	stop 95:1 98:20,25
110:8 111:10	sits 73:23 74:6	31:12 34:3 35:19	69:16 73:10 93:2	98:25 120:10
115:15 117:17	117:25 118:24	37:1 41:23 46:12	stages 10:13	stops 71:7
shape 93:16	situation 45:21,22	61:4,6 76:4 86:20	stake 39:22	storage 4:11,12 6:7
share 41:20 75:23	86:20	88:10,20 93:2	stakeholders 94:15	41:8 75:19 82:20
76:21 77:9,10,13	six 11:14,25 15:1	94:6 105:25	stamp 90:6	98:3
77:18 119:11	sizes 76:10	110:22 117:19,24	standard 22:12	store 4:3,3 9:2,4,5,6
shared 32:5 78:14	Skype 76:24 78:22	sorts 42:22	47:20 53:16 54:3	9:13,15,16,18
81:20 98:17,24	78:23 95:12	sought 6:13	97:22,24 98:6	10:5 19:2,3,7,10
108:9	sliding 101:21	sound 34:23 35:1	106:12	19:18,24,25 20:1
sharing 76:19,24	slightly 76:10 94:5	source 12:21 55:16	standards 79:18	20:2,21,25 21:9
78:12 82:18 99:1	101:7 116:2	South 97:5	Starbucks 73:4,6	22:20 23:20 25:18
110:25 111:1	small 13:23 63:13	space 63:11 66:24	73:10	25:21 34:16 42:7
shop 119:7	63:13 73:3	100:10	start 1:22 3:15 5:6	61:19,20,22 62:10
short 2:3 48:5	smaller 103:11	spark 86:23	50:25 51:12 78:24	62:18,22 63:4
71:18	Smith 74:7	speak 23:8 25:25	79:8 93:4 115:21	71:8
show 114:6	social 4:15,19	33:21,23 34:5,25	started 51:6 99:19	stored 31:10 32:8
showed 98:13	12:15 13:25 14:2	51:21 69:25	115:24	37:24 41:12,12
showing 113:19	16:22 17:4,10,16	speaking 28:2	starters 6:15	43:17,20,24,25
Showing' 114:5	36:15 37:12 61:5	73:20,21	starts 99:7 117:5	44:3,12,14,17
shows 113:5	62:2 64:13 68:21	speaks 54:8,11	state 48:16 72:3	52:5 59:15
shut 83:13	68:24 69:18,20,21	specialised 43:3	80:10,11	stores 7:3 25:17
side 8:4 63:23 76:6	society 70:3 90:13	specific 27:7 32:19	statement 1:16,18	34:15 73:7,11
signed 11:2	software 3:10,14	42:6 44:7 53:21	3:7 6:18,25 8:21	stranger 36:16

strangers 5:1 14:4 14:5,5,5,6,6,14,15	119:6	suspect's 30:24	63:21 100:19	99:20 108:21
stream 35:7,15,24	suggested 89:17	suspected 81:18	104:10	110:2
36:18 97:13 98:16	114:1	suspects 29:7 35:6	talked 36:22	technologists 67:19
98:17,21,23	suggesting 113:15	41:22	talking 34:7 71:4,4	technology 13:13
streamed 95:5	117:6	suspicious 21:10	79:15 85:15 94:2	60:13,14,17,25
streaming 78:21	suggestion 70:8	22:10	94:3 110:13 119:7	61:3,4 67:7,8,10
95:13 96:11,24	114:13	sworn 1:8 71:25	119:17,18	68:5 69:8 91:24
97:4,6	suggestions 62:23	system 3:21 33:15	talks 93:20	92:4 97:12 98:22
strengths 106:1	113:23	33:19	tallying 65:6	100:19 103:15,21
strictest 19:21	suggestive 10:1	systems 3:19 4:7	targeted 58:23	105:25 108:5
strictly 67:23	suitable 102:19		61:15 66:25 67:13	Telegram 21:19
string 100:22,24,25	suite 6:6 75:10 76:9	T	teachers 41:2	62:11
strings 100:25	sum 89:12	tab 1:16 50:22	team 2:1,3,3 3:3	Telegraph 113:4
strong 7:22	summarise 98:8	59:17 95:23	5:10 7:7,8,9,11,11	tell 5:12 6:4 26:4
strongly 46:19	summary 34:2	100:12 104:6	7:18,20,23 8:7,9	29:10 47:10 65:8
struck 11:25 16:15	57:23 99:2	106:3 113:1	8:14 9:6,13,19,23	73:14
38:8 39:20	summer 109:10	table 49:16 50:1	10:5,14,18,23	tend 14:12 66:25
structural 40:14,16	sun 74:23	51:17 52:1 54:12	11:4,10,13,14	71:5 87:8
structure 79:4	Sunnyvale 7:12,16	54:17 55:23,25	12:8,13,22,22	tens 84:20
80:21	supplier 12:13,21	56:6 57:1,9,21,22	13:23 15:2 16:4	term 4:22 53:14
structured 40:1,6	17:23 18:4	57:24 92:1	16:16 17:24 18:22	94:14 113:24
study 29:23 30:6	supply 13:3 40:3	tackling 84:24	18:23,25 23:18,20	115:20,25 119:16
58:18 96:4,8	64:10 65:23	86:12 91:17	26:21 27:1,1	119:18
subject 17:18 19:19	support 13:9,14	112:17	29:14 35:21 42:21	terms 3:11,18 7:24
23:22 26:3 38:7	27:23 45:11 46:19	tag 111:3	42:21 43:3,8,11	13:5 14:24 15:4
44:17 61:21 68:6	86:10 89:4 94:8	take 1:18 3:17 9:19	46:6 53:13,24	18:20,23 20:20,24
subjectivity 61:1	94:13,14,16,17,21	10:10,13 13:21	54:4 63:12,12,21	20:25 21:1,3,13
sublicensing	94:25	18:2 24:17 29:7	63:21 72:12 74:19	22:18,20 25:6,25
105:17	supporting 85:3	38:14 60:6 61:25	79:17,17,23 80:15	29:25 32:18,19,19
submit 30:14	suppose 62:15	64:5 65:18 69:3	81:5,11,11 84:21	37:20 42:3,3 49:3
submits 44:25	sure 4:8 6:3 16:25	77:7 78:16,17,20	86:9,14 90:22,25	52:22 58:14 63:22
submitted 9:14	18:19 19:3 26:2,2	78:22 82:10 83:6	team's 8:18 26:16	64:21,25 65:24
19:24 20:15 56:3	28:16 32:20,21	92:22 100:21	teamed 106:10	69:8,8 71:1 72:10
suboptimal 116:6	43:8 60:24 63:16	101:15,16,23	teams 14:21 17:21	85:15 86:25 87:5
subscribe 36:3	82:5,22 115:19	104:12 115:9	28:1,3 72:23	93:3 103:7 104:12
subsequently 9:5	surface 76:7,8,9	116:2,20 118:12	74:15 75:1 79:5	110:8 111:13
subsidiary 73:18	78:9 117:16,22	taken 15:25 21:15	79:10 80:20 81:13	113:15,21 114:14
73:19	119:20	69:21 83:16 106:4	83:10 86:6 91:23	114:21 115:16
subvert 21:3	surfaces 119:25	takes 12:5 13:2,10	technical 3:16 32:1	116:4,5,8,9,11,12
suffering 87:14	surfacing 111:11	15:8 55:24,25	86:11 106:8	116:18,22 117:12
sufficient 21:20,25	surrounding 34:14	63:18 65:11 81:16	107:10	117:15,19 118:12
22:3	34:15,16 64:10	85:10	technologically	118:13
sufficiently 102:2	67:8	talk 8:24 15:9	40:23	terrorists 100:5
suggest 44:13 114:4	suspect 30:25 31:1	17:20,21 24:16	technologies 85:4	test 57:2
	32:16 54:14	26:3 33:10 42:14	85:13 88:23 89:25	testing 93:2

text 37:5,9	112:16,16 114:20	tools 68:2	Tumblr 21:18	47:12 49:19 52:15
thank 4:13 5:11,24	114:24 115:13	top 48:17 51:24	62:11	52:17 54:13 55:6
7:1 10:12 14:18	116:3 117:11	52:8,16 57:1,20	turn 8:16,17 15:17	55:9,13,18,20
25:5 33:6 35:3	118:14,17 119:9	57:23 61:10	23:22 28:20 35:4	56:13,16 57:10
42:17 47:16 48:3	thinking 94:24	topic 7:7 80:19	41:5 49:15 51:15	58:12,13 59:4,20
50:23,25 51:11	103:4 118:6	91:8 112:25	59:17 61:9 68:6	68:16 72:8,12,17
52:7,16 56:7	thinks 78:21	topics 59:8	97:9 113:1,10	72:21,22 73:15,17
57:21 61:10 70:12	third 3:10 19:14	Toronto 99:17	114:13	73:18,19,20,22,25
70:15,16 71:11,16	27:5 54:7 56:5	total 26:18 50:17	turned 48:15	74:2,12,16,20
71:23 105:14	64:15 83:11	totals 50:14,15 56:7	turning 71:23	83:18,22 84:3
113:11 120:11	third-party 4:5	tracking 42:19	turns 66:4 100:22	86:6 88:15 96:20
theft 8:3 26:22	19:5,16 96:23	tracks 81:24,25	tutorial 24:20	111:20 112:11,19
theme 63:9	Thorn 67:6	119:13	TV 3:25 32:7	UK's 58:2
thing 26:11 27:20	thorough 23:16	trade 14:8 67:17	tvOS 3:25	UK-based 43:16
64:3 103:21	63:8	trafficking 2:16	twin 81:24,25	ultimately 74:7
104:16 118:16,20	thoroughly 22:9	67:11	Twitter 107:17	111:23,25
119:9	thousands 79:14	train 60:23	two 1:18 52:19 59:8	unable 33:16 84:14
things 3:9 9:10	84:20,25	trained 9:23 18:22	62:9,12,12 75:8	unclear 47:3
10:1 14:2 20:20	three 3:9 59:25	42:22 59:4	76:25 81:24 83:10	uncovered 119:5
21:2 22:2 24:23	60:4,6 115:23	training 30:7,8,10	83:10 102:11	uncovering 114:18
31:5 39:6 41:15	three-month 96:6	30:11 31:24 58:13	115:22	underlying 32:13
54:23 60:15 64:12	throw 65:2	58:22,25 59:1,5,5	two-day 92:11	56:21
73:9 76:11 93:19	Thursday 120:14	59:6,8	type 11:7 14:10	underneath 22:11
108:17 116:19	time 1:17 2:7 9:6	transactions 34:17	17:5,9 22:22	understand 6:14
117:5,5 118:22	9:16,18 15:24	35:14	59:10 63:17 78:3	14:19 25:15 29:22
119:14	18:15 19:7,11,23	transparency 50:5	115:24	29:24 42:25 44:23
think 11:16 12:6	20:5,7,14 24:6,11	50:21 57:19	typed 113:22	58:13 67:20 70:25
16:20 17:20 27:9	26:20 47:10,13,17	traumatic 11:1	114:15	89:19 92:10 94:23
29:23 39:20 40:18	50:16 53:21 62:10	treated 68:23	types 2:11 3:19	95:10 99:23
51:9 63:9,11	62:18 80:4 81:13	tremendous 12:18	11:8 19:21 24:10	100:16 101:14,19
64:11 69:10 72:6	81:24 87:23 95:14	tried 100:6	29:6 30:12 38:20	111:16 114:10
72:20 73:16 74:2	114:19	tries 98:23	59:14 75:2 78:25	understanding
75:7 76:2,17 77:6	times 9:17 20:14	troughs 87:12	80:3 88:12	35:22 40:23 46:7
79:9 80:7,17 85:2	98:18,24 100:15	truly 60:19 90:6	typically 20:12	46:15 49:11 52:24
86:3 87:18,22	timescale 93:8	trusts 32:12	75:10 76:15,20	55:19 58:20 60:16
89:14,16 90:1,5,9	timetable 93:19	truth 39:12 108:2	78:5,14 80:5,9	60:22 68:1 110:6
90:14,18 91:9,19	tiny 17:11	try 21:1 30:18 73:5	81:4 85:7 86:9	110:18
92:7,11 93:1 95:2	tips 112:2	80:2 88:8 100:8	96:14	understands 68:8
95:6 96:6 98:21	title 1:23	100:15 101:5,13	typing 115:21	115:19
99:7,17 100:3	today 106:16	103:22 108:7	<hr/> U <hr/>	Understood 21:8
102:10,17,18,25	today's 120:10	119:19,20	UK 4:9 6:15,16,19	24:24 29:18 30:22
103:3,11 105:15	told 75:15	trying 30:19 79:6	6:24 7:2,4 11:20	32:14 33:6,24
106:5 107:18	tolerate 90:13	89:19 99:23 108:4	11:23 16:6,14	34:22 37:10 42:6
108:20 109:9,15	tool 67:15,20 68:1	114:19 117:7,8	43:3 45:4,14	46:9 53:18 55:15
109:17 111:19	71:9 97:18	120:7		62:14

<p>undertaken 60:1 unfortunately 40:22 unit 79:24,25 80:1 80:17 86:25 87:2 87:5,19,23 United 2:15 56:20 56:23 67:6 83:22 units 27:3 unknown 104:19 unrealistic 93:18 update 20:15,21 92:17,25 updated 9:6,16 20:7,8,12,14 102:14 upload 96:22 97:18 uploaded 60:9 105:10 106:22,25 120:5 use 5:2 6:13,16 20:25 25:7 27:4,5 28:3 31:19 35:4 36:11,15,17,25 38:4 41:16,20 61:4,18 64:25 70:22,24 71:1,4,5 78:11 85:7 88:8 92:11 97:17 102:17 103:9 106:11 107:19 108:3,5,8 useful 100:18 102:23 user 36:3 37:23,24 41:9 43:14,19 44:2 61:6,8 81:21 83:16 102:15 117:8 user's 82:13 users 4:22 6:21 11:23 16:14 43:17 53:21 100:8 102:20 104:22 114:6</p>	<p>users' 39:21 107:5 uses 31:4 64:6 108:21,24 usually 22:15 utilising 21:3</p> <hr/> <p style="text-align: center;">V</p> <hr/> <p>valid 53:7,12 valuable 95:7 value 17:13,14 67:9 68:22 102:8 118:15 valued 69:16 variety 4:2 7:3,23 7:25 22:2 various 2:20 4:19 6:19 7:10 28:5 29:4,6 36:14 39:15 42:12 50:2 74:24 75:1 80:3 86:18 88:9 94:9 94:14,18 114:9 verify 23:4 versa 84:4 version 33:9 versus 66:16 vice 84:3 victim 70:6 96:11 96:12 victims 67:11 video 5:13,21,23 36:2,8 41:20 76:19 77:9,13,21 77:22 95:20 97:12 97:23 98:6 99:5 101:8,10 104:3,5 104:9,11,13,24 105:9,12 113:25 videoing 77:12 videos 78:15 96:5,8 96:13 97:1,24,25 103:25 104:4,5 105:5 view 12:9 23:13 35:14 38:17 39:5</p>	<p>110:13 119:11 views 68:11 violation 22:18 23:1 viruses 80:8 visibility 23:5 24:1 24:10,13 56:21 volume 47:18 voluntarily 46:13 volunteered 11:7 VPNs 68:5 vulnerable 14:9 37:16</p> <hr/> <p style="text-align: center;">W</p> <hr/> <p>wait 70:13 waiting 66:3 walk 19:16 want 17:25 19:17 38:19 51:21 74:10 82:22 83:6,8 93:17 100:3,15 101:13 103:12 112:17 115:19 118:10 wanted 70:20 90:6 94:22,23 95:13 99:14 100:5 107:13 wanting 30:24 warrants 42:10 Washington 3:2 wasn't 52:25 97:3 watch 3:24 36:14 94:20 watchOS 3:24 way 8:22 13:5 19:23 38:4 39:17 40:1,6,12,20 60:20 64:7 84:7 88:2 93:23 96:3 98:9,21,23 100:5 102:22 103:3 104:20 112:16 115:12 116:3</p>	<p>118:2,6,7,22 ways 13:20 39:7 65:20 86:11 119:12 we'll 4:13 18:18 48:2 71:15 76:6 85:12 we're 1:7 3:11 12:15 16:24 31:14 49:8 59:6 62:23 64:2,2 69:11 71:23 73:8 80:18 85:15 90:15,16 91:14,14 92:6,24 94:3 95:12 100:9 111:8,9 112:17,20 118:6,21 119:17 119:17 we've 13:4,13 18:12,22 20:8 21:14,14,16 27:10 29:21 32:15 36:22 59:3 66:19 67:5 82:22 83:17 92:20 92:21,22 94:19,20 94:22,23 96:2 104:2 108:11,25 109:15,16 117:23 117:24,24 118:5 119:16 wearing 101:25 web 67:12 120:5,5 webcam 97:2 website 24:19 25:9 25:15 websites 96:23 Wednesday 1:1 week 9:17 20:14 47:21 73:9 weeks 17:2 92:25 welcome 1:4 22:7 102:17 went 71:20 87:22 120:22 WePROTECT</p>	<p>118:25 weren't 68:2 115:12 western 97:6 whichever 1:20 83:25 whilst 97:21 115:4 whistleblower 13:15 White 66:9 68:7,12 68:17,18,20 69:1 69:5 86:7 Wi-Fi 73:9 wide 7:23,25 102:7 widely 24:25 wish 40:20 83:17 witness 1:8 wonder 98:8 120:9 wondered 93:23 105:9 word 75:11 85:5 115:22 wording 117:6 words 20:22 37:21 115:23 work 2:7 7:7 8:10 8:18 11:7 12:1,24 13:3 17:22 18:21 28:3 30:9,14,17 32:2 58:24 63:24 72:14,16 74:23 79:11,17 80:13,15 87:5,11 88:3,21 90:5,17 92:2 94:19 95:6 118:22 work-around 45:13,16 worked 2:12,15,16 2:20 9:22 11:4 21:21 67:15 73:4 118:5 working 11:6 63:12 65:9 66:23 72:24 73:3 81:8 86:22 98:5 118:15</p>
--	---	---	--	--

works 29:19 60:21 100:11,16,20 104:9,11 108:12	96:16	2.4 38:10	400,000 27:10	8.6 43:13,19
world 11:18 12:18 16:7 30:7 39:16 65:20,23 74:15,25 85:3 88:7 107:15	<hr/> Z <hr/> zero 56:13 57:5,16 zoom 57:20 61:10	2.55 71:21	45 99:8	8.7 43:13 44:13
worldwide 6:17 7:9 11:22 12:1 16:8,9 16:17 51:18 57:22 58:22 73:24,25 103:16	<hr/> 0 <hr/> 1 <hr/> 1 6:17 120:18,19,21 1.45 71:15,19 10 23:23 109:19,19 110:15 10,000 65:13 10.30 1:2 120:14 100 16:5 23:18 90:7 96:21	20 8:8	47 105:7	8.8 47:15
worth 90:18	11 57:19 79:8	2008 99:17	4x4 83:24 84:6,7 114:21 115:4	8.9 47:15
worthwhile 95:19	11.40 48:4	2009 99:12 106:13	<hr/> 5 <hr/> 5 15:10 59:18 61:10 113:1	849 56:11
would've 55:14 103:23	11.55 48:2,6	2012 2:18 72:25	5,000 73:16 74:1	87 57:14
wouldn't 45:3 51:16 55:5 89:9	110,000 73:25	2013 50:15,20 51:10,11	5,800 81:4 109:10	89 58:7
written 118:9	12 87:3 114:3	2014 34:23 109:10 109:13	110:17 111:16 112:8,10	<hr/> 9 <hr/> 9.2 66:21
wrong 12:6,8 30:16 35:1 46:25 103:23	12.35 71:17	2015 50:17	5,800-monthly 109:7	96 96:13,17
<hr/> X <hr/> X 120:17	1239 56:10	2016 105:16 106:5	5.6 19:9 20:17	97 57:8
Xbox 76:8,14,18 77:6,6,17,19 78:16,20 82:19 110:25 111:3,9,11	13 70:21 96:16	2017 2:23 28:15 50:15,20 96:7	50 105:15	98 96:15
<hr/> Y <hr/> Yahoo 107:17	13' 114:2	2018 28:14,17 50:21 51:4 52:18 59:21 95:2 109:14	500,000 27:10	
Yeah 112:21	15 1:1	2019 1:1 118:9 119:3 120:14	51 107:20	
year 16:4,16 23:19 26:4,17 27:9,13 27:23 28:13,14 29:23 65:13 67:3 81:5 89:23 91:22 92:9 109:19,19 113:4 114:3 119:4	15,000 49:20,21	206 54:17 55:1	57 111:5	
years 16:10 28:12 49:20 93:21 94:2 96:16 109:20	155 102:16 103:15	2397 56:8	<hr/> 6 <hr/> 6 8:21	
York 2:13	158 56:8	24/7 47:23	6,500 7:1	
young 77:7	16 48:18 96:25 120:14	25 108:14	<hr/> 7 <hr/> 7 51:15	
younger 76:22	17 21:17 109:18 110:15	250,000 67:4	71 120:22,23	
	170 86:21	263 52:18 55:8,16	72 120:24,24	
	172 58:2	28 52:19 54:12	73 96:24	
	18 6:22 94:10 97:10 109:9,10	<hr/> 3 <hr/> 3 1:4 104:6	77 58:4	
	1977 3:5	3.6 18:1	78 57:10	
	1997 73:16	3.7 27:16	<hr/> 8 <hr/> 8 33:13,14,15,25 34:3,22	
	<hr/> 2 <hr/> 2 26:19 100:12	300,000 28:9,10	8.12 48:10,18	
	2,082 96:8	300K 28:17	8.13 33:7	
	2.1 3:7	32 57:6	8.14 51:9,10	
	2.2 6:25	33 57:4 92:7	8.17 49:15	
		365 75:7,8,10,11,15 75:20,25	8.2 53:2	
		<hr/> 4 <hr/> 4 59:18 72:20 96:23 106:3	8.20 53:9 54:7	
		4.05 120:12	8.22 58:16	
		4.1 15:7,10	8.23 58:16	
		4.1.3 8:21	8.3 28:22	
		40 58:3 96:18 109:8	8.4 42:15	