

Tuesday 11 October 2016

[Watch the meeting](#)

Members present: Lord Best (The Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bonham-Carter of Yarnbury; Earl of Caithness; Lord Gilbert of Panteg; Baroness Kidron; Baroness McIntosh of Hudnall; Baroness Quin; Lord Sheikh; Lord Sherbourne of Didsbury

Evidence Session No. 3

Heard in Public

Questions 37 - 51

Examination of witnesses

Mark Donkersley, Managing Director, e-Safe Systems Limited, and Professor Derek McAuley, Professor of Digital Economy, University of Nottingham.

Q37 The Chairman: Welcome to you both. Thank you very much for joining us. As you know, we are deep into our inquiry into children and the internet. You are billed as our technical experts today and we are very grateful to you for coming and being just that. I am going to ask you, if you would, to briefly introduce yourselves. Perhaps, Professor McAuley, you could explain the main aims and the methodology you use at Horizon, in particular the work that you do with youth juries. When I come to you, Mark Donkersley, if you could explain a bit more to the Committee about your company and the system it provides, how the systems work, how your company is funded and so on, that would be helpful too. Introductory statements, if you would, starting, Derek, with you.

Professor Derek McAuley: I am a professor of digital economy at the University of Nottingham and for the last seven years there I have been running a research institute into the digital economy. Within that context, which is quite broad, we have been looking at the opportunities and challenges in the use of personal information. That is the context for Horizon. Obviously, to build an inclusive society, we have to deal with the digital economy for all age groups, so we are interested in not just the compos mentis 25 year-old single adult, which a lot of the technologies are targeted at, but children and disabilities, all sorts of things, to build an inclusive society. To that end, we had a particular project looking at social media analytics, something I gave evidence on to the House of Commons Select Committee.

In that context, we used youth juries as a way to elicit from children and young adults what they thought of social media. The methodology is to present vignettes, so you presented them with short dramas enacted sometimes in front of them, sometimes with a video, which presented

some form of dilemma; for example, personal data tracking, issues of concern around removal of embarrassing or inconvenient content. These were presented as vignettes, and the jury, composed of 10 to 15 of the children, mostly aged between 12 and 17, were then asked to pass judgment. They did not sit quietly at the back of the room; they had to discuss it. It was an experimental methodology to try this, rather than to have what would normally be a focus group based on a vignette. Calling them juries and having them making decisions was an important part of that process.

There were three in each of three cities, so there were nine juries all together, in London, Leeds and Nottingham, and in fact they were focused around the 5Rights, which Baroness Kidron has been championing and leading. We partnered with the then iRights group to do this work. From that, this is the evidence we have, we have presented it in written form, and I will answer questions in detail as we go along.

The Chairman: Excellent. Thank you very much. Mark Donkersley.

Mark Donkersley: Good afternoon. I am Mark Donkersley, managing director of a company called e-Safe. I have had some 30 years in the IT sector and since 2009 have been working to develop an operation currently based in Salford, Greater Manchester. Our task is to deliver early warning and safeguarding risk, predominantly into the education sector. We monitor approximately half a million students and staff in the UK from Salford. We also have a much smaller but nonetheless important group of school and college customers in Australia.

Our service is basically a combination of technology which is deployed to the school or college devices; the school environment. That technology is effectively watching the material coming to the device screen—so your laptop, what images are appearing there, whether they are moving or static; it is looking for pornographic material in that sense. It is watching the words and phrases coming to the screen, it is looking at the keystrokes entered into the device, and it is looking at material and activity conducted from connecting devices, so pen drives, downloads from mobile phones, that sort of thing.

When the technology detects material it feels is inappropriate or it matches what we call our threat libraries—these are literally tens of thousands of terms, phrases, euphemisms, slang, in multiple languages associated with a range of behaviours, whether it be paedophile grooming, child abuse, FGM, bullying, self-harm risk and so on and so forth—if something triggers, we receive a screenshot of what the user was looking at on the screen at that moment. That screenshot is reviewed by a team of multilingual behaviour specialists, as I say, based in Salford, and they will review that incident in context and, depending on what they believe is going on, they will escalate that incident if necessary to the school or college, going through to nominated contacts—it could be a head teacher. If it is illegal or life-threatening, the incident is rung through in real time, so something detected now, at half past three in the afternoon, is going through to the school at half past three in the

afternoon. There is then a protocol that is tiered down so that you have still serious but not life-threatening or illegal incidents sent through the same day on encrypted reports, and down to lower level material which goes through weekly and monthly.

We perform that function also for a number of UK police forces. With regard to the police, we are monitoring sex offenders who have been released back into the community where the courts have determined that they should be monitored. Clearly, there we are exposed sometimes to grooming activity, certainly child abuse imagery, and I suppose the differentiator, the reason why the police and schools use us for the service I have described is that we apply specialisation; we remove the burden of a school or police officer attempting to look through this material and identify whether there is a risk that needs escalating. We are performing that function for them.

We are a private company, funded privately with the exception of additional funding from Greater Manchester, which wishes us to grow our international monitoring unit within the confines of Greater Manchester. That is e-Safe.

Baroness McIntosh of Hudnall: What I struggled with a bit, Mr Donkersley, when I was looking at your evidence was that I could not immediately—this, incidentally, is not the question that is written down in front of me, so forgive me if I pick up on something else. Could you say something about consent in relation to the monitoring that is going on, and also, where the content that you are viewing or monitoring is evidently self-generated, that is to say, the child or young person is creating it themselves, do you have a different view of that from the view that you would take if it were material coming in from outside? Can you also talk a bit about what happens once you have notified a school that something that your protocols regard as untoward has occurred? Do you advise the school about how to take that forward? What do you expect them to do with the information that you provide to them? What, if any, redress or appeal system might there be for a young person who feels they have been, for example, unfairly targeted?

Mark Donkersley: First of all, with regard to the education sector, we are monitoring behaviour on school devices and in the school environment. A student in the UK will have signed up to a code of conduct, an acceptable use policy, which determines what they should and should not be doing, what is allowed and what is not allowed on school equipment, in the school environment. At that level, we are not monitoring a personal device per se, unless it has been brought into school and is now being used in the school environment. We are delivering a service which is addressing or helping to address the school leaders' and chair of governors' statutory duty of care regarding safeguarding and protection.

Baroness McIntosh of Hudnall: Can I stop you for one moment, just to fill in one particular blank? Is it purely voluntary that the people who access your service choose to avail themselves of it and, if they do,

presumably they pay for it and that is a discretionary choice that they make from their school budgets, is it?

Mark Donkersley: Correct. There is now statutory guidance from the DfE which in theory compels schools and colleges to provide appropriate monitoring, without really being too clear about what appropriate monitoring is. You are correct: a school determines that the early warning safeguarding service that we can provide is something that they require; they see value in it; they purchase that from e-Safe.

Regarding the material we are looking at, to some degree the individual is anonymous. What we see is a user ID, so not "John Smith" but a user ID. We see that user ID has worked on a particular device—Laptop 01—and at a particular time and date they have viewed a pornographic image, bullied somebody, whatever. Often we will not know whether it is male or female. That degree of anonymity also gives us objectivity in the review process. One of the challenges for schools, if they were attempting to do this internally, is to say, "Oh, it's John Smith again. He's always doing this—ignore it." We review absolutely every incident. What we are looking for is not necessarily the obvious material; it is what we call the ones and twos. What I mean by that is, if you look at the behaviours we detect, invariably the markers are incredibly subtle. FGM does not take place in school but young people on occasion will leave a marker, albeit subtle, about a concern they may have which is one or two steps removed from FGM, but with our specialist review we can say, "Right, OK, there's a potential risk here. This looks wrong", and escalate it through. We have that objective approach.

When we find something, we basically inform the nominated individual at the school. As I said earlier, if it is illegal or life-threatening, invariably a head teacher will be on the escalation list. Bearing in mind we are doing this throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday in the UK, the proportion of incidents which are very serious during that period is much higher. We are currently probably looking at 12,000 serious incidents a month across all our schools. When you look at the school holidays just gone, we were probably averaging something like 200 serious incidents a week. A high proportion of those were illegal, life-threatening, and therefore, again, we are filling a gap that a school would find very difficult to meet regarding attempting to monitor behaviour, and what has happened there is the devices have travelled home with the student or the staff member—because we are monitoring staff as well.

Q38 Baroness Quin: The question really is about trends and changes recently. I think we would like more information about what kind of harmful or potentially harmful behaviours you have encountered during the monitoring and if there has been an increase in different, specific

types recently, and if there has been such an increase, to what do you attribute that?

Mark Donkersley: In the written evidence we submitted, we illustrated that at secondary level there has been almost a doubling of the volume of incidents that we have been reporting and escalating back in, and it is an across-the-board increase, across all behaviours. The areas which probably give us most concern regarding increase are products such as Chatroulette. I am not sure if the Committee is wholly familiar with Chatroulette, but in very simplistic terms, these are applications—I am sure Derek can explain it technically as well—where a user basically goes online and says, “Hi, I’m Mark. Is there anybody out there who wants to talk to me?” You can imagine that you end up anywhere in the world talking to anybody. You might find yourself in the middle of some online sex act or, as we have detected, directing child abuse behaviour in some other country from your position on your laptop. The Chatroulette sites are figuring highly in the more serious behaviours around sexting and abuse. They are also the more difficult ones to trace. Clearly, we know that a staff member or a student was on this end of the chat sequence, viewing whatever or conducting whatever. It is very difficult for the authorities to trace the other party, which can literally be anywhere in the world.

Are there reasons for the increase? We see a lot of circumvention of security. What we are looking for, the behaviours that we identify, are not new; they have always been around. Clearly, the digital environment today offers, maybe with some of the behaviours, a vehicle to make it easier to conduct them or whatever, but we work on the basis that at technology level it is impossible to protect completely: no matter how high the wall is, whether you have barbed wire on the top, people find ways through it, under it, over it, whatever. Our expectation is that someone will circumvent this, and because of social media in particular, when circumvention occurs—and here another term is very prevalent, proxy avoidance—with proxy avoidance, you are basically going to a very benign website, which becomes a launch pad for anywhere on the internet. Every school in the UK and many schools abroad put in what we call edge-of-network filtering systems. These are looking at the broadband feed and they are looking out for things such as proxy avoidance, as well as blocking material from *Playboy* or whatever it happens to be.

With regard to proxy avoidance, there are certain standards that these sites conform to and usually they are picked up, but these things are being created daily all over the world. What we find is, for instance, on Monday this week we picked up proxy avoidance sites we had never seen before. They could have been created at the other side of the world but the social media engine has got through—people have identified this and said, “I’ll go and try it out in school today”. Basically, what it allows you to do is completely bypass all the security, and once you are on the proxy avoidance site you can do literally anything and nobody can, in theory, see what you are doing. We can, because we are looking at the device, so

we can see that the person has put a bet on the 2.30 at Kempton even though betting is not allowed in school; we can see that they have looked up pornographic material, or whatever it happens to be.

We are seeing an increase in proxy avoidance sites which the edge-of-network filtering systems are not trapping. We will report it to the school—so we report, “Someone has looked at pornography and they have been on a proxy avoidance site. It is called XYZ”—and the technicians in school will no doubt run off and put that in to block that site, but then another one pops up. It is a viral network through social media; people very quickly hear about these, they know which ones beat the system, and they start using them, and then they are looking for the next one.

Baroness Quin: I understand that obviously you report back to the school or college or to the police force, but if in the course of your work you have general concerns because of the rise in a particular kind of activity, do you report that to anyone? What do you do, apart from coming to speak to us, with your overall concerns rather than your relationship with particular schools and police forces?

Mark Donkersley: Our service is confidential to the target customer, the school, so we do not divulge and discuss the detail of what has been going on there. Yes, we do generate analysis of behaviour, our experience of monitoring currently half a million students and staff, and we are incredibly keen to share that material with policymakers and whoever else feels it is worthwhile for them. Our aim is to safeguard and protect, that is what we are passionate about, and that is what we are doing for our customers but, as in sessions like this, we believe there is information that we can provide that can assist whether it be policymakers or just the general understanding of what is really going on out there, because we have this unique window. We are not inviting people to tell us what they think is going on and fill out a questionnaire; we can see it. We know it is happening and we know it is happening to that volume.

Baroness Quin: I also ought to ask the second part of my question, which was: do you see any evidence that harmful behaviour associated with the internet disproportionately affects girls?

Professor Derek McAuley: We have not engaged in this sort of monitoring. The scale of what we have done is qualitative data, which I would not like to go on record as saying definitely shows one way or the other; it would all be anecdotal. We simply have not done that.

The things that one can do legally and that Mark is talking about I would not be able to get through a research ethics committee at my university. I would not be permitted to do that research.

Mark Donkersley: Unfortunately, for the reason I mentioned earlier, in the main we do not know whether it is male or female, unless we can see

through the evidence of the actual incident, or it is reported back to us, "That was a female student" or "That was a male member of staff."

Baroness Quin: Do you have any anecdotal feeling about it?

Mark Donkersley: Anecdotally, we would say that the gender which is on the receiving end of a lot of the sexting-type behaviour is definitely female. It is female images we are seeing being passed around. That is not to say there are not male images as well but it is predominantly female.

Q39 **Baroness Benjamin:** I would like to move to age groups. It has been stated that children and young people have significantly different capabilities and expectations. In the course of your work and the research you have done, do you see notable differences among the various age groups, and is there adequate knowledge and expertise within the industry to address the needs of children of different age groups, between, let us say, zero and 18?

Professor Derek McAuley: Seven minutes before I came into this room there was a Twitter message: 67% of under twos in Sweden are online, which was announced at a workshop today. That is a fairly spectacular number. I think, having watched some of the evidence previously. This is where the issue of trying to draw a very hard line and saying there is a certain age at which suddenly everything is understood by a certain child is—and I am a technologist—socially not sensible. Children develop at different rates. What they are sensitive to is highly context-dependent. We have an example of a six year-old girl becoming very upset simply by seeing an advert about Ashley Madison, the dating website for married people, because her parents had gone through a divorce. The thing that will actually upset very small children does not have to be illegal and it does not even have to be something that you might view as something that should be banned, but it is something that upsets that child.

The industry has done nothing to address tools that would allow much more subtle voluntary filtering. Most of the work we have done goes down only to five year-olds—again, we would have a real challenge if we tried to research younger than that—but five to 10 year-olds are mostly concerned about not seeing things they do not want to see. They are not out there trying to find things. One of the challenges they have is that if something happens to them, they do not know where to go; they do not have a safe place to go and ask about it, for fear that it would be seen that they have done something wrong. That in one sense also extends to the parents; they have a fear of discussing these things with parents. As a technologist, in my village I happen to receive lots of requests: "Can you come and clean up this PC because my son won't show it to me?" I will go and do what is needed and explain to them why they have all this malware. Most of it is because they were trying to download free games but there is a lot of other content they do not want, and they do not feel they have somewhere safe to go for advice.

There are a number of things here. There is obviously illegal content, and you have heard evidence about how to deal with that. There is content that is inappropriate in different contexts. I think we have done very little to deal with children being online, all the way from the tiniest, the 67% of under two year-olds. People are giving them tablets and just saying, "Here you go."

One of the comments I would make which calls back to the previous question about harms is that the advice used to be to keep the computer in a public space, but those computers did not have cameras in them, and there tended to be one in a house, whereas now every smartphone—and the kids are demanding smartphones earlier and earlier—has a camera. It has two cameras: one so you can see the screen and one that points at you. The technology we are putting into kids' hands that they take to their bedrooms is one of the things leading to a wave of these new apps that have this particular behaviour. All the common-sense advice we have about using technologies in a public area so that people can see what is going on and there can be discussion is just not happening. The danger is that, without some action by the industry to put in place mechanisms that protect the youngest children from things they really do not want to see—not that they are illegal or anything else, and that includes issues such as safe search. Age-appropriate search would be a revolution, and it is not beyond the wit of great scientists in those search companies to figure out.

Baroness Benjamin: In the light of your work with children, do the different age groups understand their rights, and in some cases realise that they are breaking the law by sending inappropriate imagery?

Professor Derek McAuley: I fear that most adults do not understand their rights when it comes to online platforms. How many of you read the terms and conditions? The basis of informed consent as the basis for all data processing is somewhat flawed, to say the least. There is a fundamental problem in that certainly in terms and conditions—and you saw in some of our evidence children talking quite eloquently on terms and conditions—the reading age is often 21 or 22. It requires undergraduate if not postgraduate education to read the text—not to understand the law and the legal implications. I do not think the kids understand it. They sort of know something they are not supposed to do at 13 because it says something about 13 in there but also I think a lot of them do not even think about their behaviours. The classic one that comes from the Chatroulette would be young girls dancing in front of a camera in their bedroom, semi-clothed. That would be something they might not even think about but it is harming themselves long term, and who knows who is at the other side of that conversation?

There is a real lack of understanding around these issues, and the repeated dangers of the internet. One of the lessons that came out very strongly and one of the reasons kids liked our youth juries was that they were a different way of getting the message across, an entertaining way. The way I would put it is we have a world-class creative industry; it

should be doing something about communicating this at every age group. There should be a plot line in “East Enders” or something, or whatever kids watch. It is that sort of thing that I think is important, to get age-specific information to people, but also through channels that they will enjoy.

Mark Donkersley: I would certainly concur with Derek’s comments there. I think the point I would make across all of certainly the primary and secondary sector in the UK is that the issue we have seen for many years now is mental health. We put in the evidence that that has massively increased but it has always been there. When you look at the various independent reports that have been done for NHS England saying that 50% of mental health issues are established by the age of 14 and 75% of mental health issues are established by the age of 24, that is squarely within that primary, secondary and further education group. The volume of markers that individuals will leave in the IT environment is incredible to us. They are subtle; they are not the in-the-face pornography or anything like that; these are either cries for help or the very low-level things going a bit awry at home, “I don’t feel comfortable”, the depression indicators, that sort of thing. We would say it is in that area. If you look at primary, across all behaviours, you see much more change over time. We genuinely believe that is because of the age group and because of the early warning of the risk, and the fact that teachers are then able to intervene, they can modify the behaviour. They have a much greater struggle doing that at secondary level because of the age of the individuals.

We also see that the age group is lowering regarding skill set and use. You used to think it was the elder siblings at secondary telling their primary school siblings new ideas and ways and things that maybe they should not be doing on the internet and with digital equipment; now it is almost the other way round, that primary age is informing secondary. They are coming up with the ideas, which is incredibly dangerous, obviously.

Baroness Benjamin: You mentioned protection. What are the key technical challenges about protecting, when we talk about protection, especially with age verification? A lot of people say it cannot be done, you cannot do this, you cannot do that, but what challenges do you think we face in trying to protect children through age verification?

Professor Derek McAuley: Mark has already pointed out that there is no technology that someone smart cannot get around. It is always a bit of an arms race. The other side of this is that I would be deeply concerned that most of the systems proposed—and there was a report very recently—involve convincing people to hand over personal information to a random website in the hope that it verifies their age, when in fact that is one of the things we should be teaching people not to do, to go to a random website and hand over credit card details or something else. The various mechanisms proposed are somewhat dubious.

I would look at something such as UK Verify, which was set up by the UK Government as the way to do identity for all government services. It has been rolled out already for universal credit, and asked of that group. It was not designed for age verification but that was co-designed with the civil society organisations, which have a concern for privacy, and it passed their test for identification. I would start from something such as that as a way forward. Many of the, let us say, commercially proposed ones, are deeply worrying—and I say that as someone who spends most of their life trying to avoid these people tracking me, and that is what I have taught my children, because being tracked is just as bad. The age verification mechanism becomes very difficult in a world where one also wants some privacy, not necessarily for dubious reasons, but just because I do not want them tracking me all the time. I think there is a challenge there. I have yet to see a solution that is satisfactory but, as I always say to my research students, until you have proved it is impossible, it is still possible, so you should keep looking.

Baroness Benjamin: They can track you if you want to gamble or you buy things on the internet, so what is the difference?

Professor Derek McAuley: Okay. I use a different identity for every service I use, so I have hundreds of email accounts. I also take measures in my browsers to stop them tracking me. It is perfectly doable. In fact, Microsoft nearly made it the default but the advertising industry went after them and shut them down. Tracking is something that one can avoid, but as soon as you say it will become a legal requirement for people to track, then those of us who value privacy over the convenience—which is all it is, because I am perfectly capable of using these services individually but I refuse to be profiled across everything I do.

Q40 **Baroness Bonham-Carter of Yarnbury:** From tracking to filtering, please. Does the present regime of filtering protect children adequately at school and at home? We had some written evidence that when parents decide to use a child-safe filter service from their ISP, the filter will only apply to the smartphone if the child is connecting to internet at the home, not when the child is connecting via the mobile network. It does not sound as if filtering is a very satisfactory way of protecting children from content.

Mark Donkersley: It has a place, definitely. It has an ability to effectively close the tap, but it cannot close it completely. We have talked already about circumvention and proxy avoidance, for example, as a way of circumventing filtering. The challenge with filtering is obviously to have the balance there to allow the user to exploit the power of the internet and at the same time protect them from the risks and dangers.

Baroness Bonham-Carter of Yarnbury: I am sorry. There is something I did not understand there. Is the child trying to overcome the filter? Is that what you are saying?

Mark Donkersley: Oh, yes.

Baroness Bonham-Carter of Yarnbury: The child knows that his parents have put a filter on?

Mark Donkersley: Potentially, yes, but this is where monitoring at the device provides the belt-and-braces approach, because even if it is circumvented, or, as you said, you step into a different environment and the filtering is no longer there, the fact that the device is being monitored allows you to identify that that individual is now looking at "Call of Duty" and they are only six, whatever it happens to be. It goes back to the earlier point as well, I think, that age verification itself is not the biggest challenge in the world, as Derek says; there are ways and means but people will find a way round it, but if you are monitoring as well, that is what is telling you someone is gambling at the age of 10 or someone is going on to Facebook when they are three. The evidence is there. The challenge then, I would argue, is to inform the parents and make the parents appreciate the challenge.

Baroness Bonham-Carter of Yarnbury: That was going to be my next question, exactly that. Are the parents alerted to the fact that the child is using these sites?

Professor Derek McAuley: BT—I have never used one of these services myself; I would rather have a conversation with my children about it—would flag up sites visited and things such as that. There is a real danger with that, though, as a general mechanism, of showing too much detail directly to parents, and that is one interpretation, because you go to a website today and content is pulled from hundreds of machines. The adverts are coming from a completely different company, and who knows what the advert is? That is easily misinterpreted. It is one thing to have a company with experts who will disambiguate that but, again, we have not yet been able to figure out ways in which to represent the topics that the child is looking at; so rather than say, "These are the websites they went to", and leave it to a parent to try to interpret that, saying, "Your child is showing an increasing frequency of attendance at these sorts of sites" and prompting a discussion. Again, the social development is different for all children. Anyone who has more than one child will know that they have two different children, they develop socially differently, and the content that a parent lets a child have access to in the home will vary depending on whether you believe your child is ready for it.

There is a different point from the very first question. You had the Internet Watch Foundation in here, and for illegal content, and for clearly specified adult content, most public wi-fi providers and the cell phone companies implement the same sorts of filters by default that, for example, Sky do, so it is true that in many places they take the phone it will still have the same sort of filtering going on, but at that point it is strictly filtering; it is not reporting, because there is no parental-house relationship to report it to if it is a pay-as-you-go mobile.

Baroness Bonham-Carter of Yarnbury: A quick supplementary, which I think you were touching on, which is that of course you do not want the filters to filter information that is of help to young people, on sexually

transmitted diseases or whatever. That is another problem, presumably.

Mark Donkersley: It is, and certainly within schools, again, this presents a challenge, because you have on the one hand probably a vast swathe of material suggesting that individuals have been on these health sites, whatever, which at first glance may be indicating some sort of health risk, but it is all very genuine and not an issue. That is what we are saying: at the beginning the challenge that school leaders have is that they do not have the resources with the specialisation and the time, and they certainly do not have the budgets available to just sit there poring over this material, whereas we do.

Lord Sheikh: I wanted to refer to FGM. Mark, you touched on that very briefly in your introduction. It is a subject which concerns me greatly. I have spoken on this matter in the House of Lords and, more importantly, I am the co-chair of the All-Party Group on Sudan. I led a delegation to Sudan recently and we looked at issues concerning women. Following that, I am sending a group of British parliamentarians to Sudan. What is happening on FGM is, of course, this is still going on with regard to young girls in this country but also girls are being sent from this country abroad for this horrible action to be taken. You mentioned FGM. What work have you done and what degree of success have you achieved?

Mark Donkersley: We collaborate with many organisations which are specialists in the different types of behaviour. In this particular area the challenge is that it is not very obvious. Someone is not going to say, "I am worried because I am being lined up for FGM." They are not even going to use the phrase, the terminology. It is going to be a subtle, young person's way of describing a concern that they have an inkling they are actually being sent away from the UK and they think, "This is going to happen to me. This is why I'm going", and that concern is being expressed. We work internally to almost create that youth-speak, so we understand the nature of the issue, we appreciate the marker that we are looking for, and we said, "Okay, how is a young girl going to articulate a concern around this, given that they are probably not going to mention FGM?" We come up with all these different markers, terms, phrases, and that is what we look for, and when we tease them out, great.

We are also made aware by various organisations of, shall we say, the code that is being used at parent level to disguise FGM, and we incorporate those markers as well. I will not quote one here in open forum, but sometimes we might have a young person saying, "I've heard my parents reference this and I think that is code for circumcision of some description." We will find that incident, review it, and in the particular way I have described, that would be escalated to the school to intervene.

Lord Sheikh: My own feeling is that of course we have to change the culture, although of course it is a criminal offence, not only here but in overseas countries. Therefore, if a role can be played in changing the culture, I think we would have a better chance of success.

Mark Donkersley: Sure. I would also point out that we have over a million students at primary and secondary who do not speak English as a first language, and you can flick a computer now and change that keyboard to Urdu, Farsi, Polish, whatever, at the touch of a button. Often, the more serious behaviours, again, are being articulated in a foreign language, maybe Urdu script or Arabic script. We are fortunate that we can detect that. We have to make sure we have the markers in there and that we understand the cultural emphasis, and it is a major challenge for us to be completely on top of that.

Q41 **Lord Sherbourne of Didsbury:** Can I ask about the role of Government? As I understand it, the Government produced some proposals at the end of last year requiring schools to put in measures to protect children from harm online, if I am correct, and there are some proposals in the Digital Economy Bill. What further things do you think the Government should be thinking of doing? What would you like to see them doing?

Mark Donkersley: A number of different things at different levels. It is our evidence and experience that nearly a third of all serious behaviours we escalate are the result of offline activity—nowhere near the internet, no online activity at all. There is very little, if any, mention of offline behaviour and how you should be trying to interpret and monitor that in any of the guidance being put forward by Her Majesty's Government. That is an issue. Nearly a third is a big hole.

Lord Sherbourne of Didsbury: What would you like them to do exactly?

Mark Donkersley: First of all, educate the inspectorate and the school leaders that this is not just an online issue. It focuses the mind in an area; okay, it is where the majority is happening, i.e. two-thirds, but one-third is a big amount to be missing, to have invisible.

Lord Sherbourne of Didsbury: The Government should be doing what? Educating?

Mark Donkersley: Yes. In statutory guidance that has been provided there needs to be more understanding of the reality of how the digital environment is being used. Offline activity is a significant proportion of activity and there are a lot of markers there which are of value to school leaders.

I would say the second point around this is that we see what we do as a public health issue. We regard the evidence of what we see as a public health issue. We have talked about mental health, about the fact that the emphasis is on young people where mental health issues are established. The NHS is spending huge sums of money on mental health, and there are all sorts of reports out there saying that intervention at an early stage is not just going to help the individual, it will have this wider benefit and value to the NHS and other government departments. We feel that, alone, purely the issue of mental health is more than adequate

justification for the Government to be mandating monitoring across schools.

Lord Sherbourne of Didsbury: You want to have mandatory monitoring in schools?

Mark Donkersley: Absolutely.

Lord Sherbourne of Didsbury: Can I ask Professor McAuley what your thoughts are on what the Government could do?

Professor Derek McAuley: The one thing that came very clearly from the youth juries was this comment that people did not know where to go when they had a problem. We have listed all these problems that people have, "Don't do this, don't do that." It is a bit like saying, "Don't fall over and break your leg" and then fail to provide an accident and emergency service. They need somewhere to go. This applies to parents as well; the parents often do not know how to react. From all age groups, we need children to be able to feel they can go and talk to someone safely about something that has happened.

Lord Sherbourne of Didsbury: What kind of people would those be?

Professor Derek McAuley: I would hope it would be within the school system. It would be a function that would be defined, that would say, "This is the amnesty. Come here and tell us what happened and let's get this mess cleared up." Monitoring is one thing but without sitting down and doing a lot of research into what he has done—which I might find hard, getting to the heart of how much of it has started off in a small way and escalated over time; was there a point at which we could have intervened? As with mental health issues, the question is whether there is a point at which you could intervene much earlier with assistance and more engaging education. The internet is a great thing; it is not all bad. We have to be careful.

Q42 **Earl of Caithness:** Can I take you on to data protection? Does increased monitoring of online activity have implications for the data protection of children? Is that going to change with the EU regulation due to come into force imminently?

Professor Derek McAuley: Absolutely; it is a data protection issue. The GDPR brings in tighter constraints on consent and the types of information that are considered personally identifiable information. If I look at the industry in general, they get away with it on data protection. In some countries they are quite hot on enforcing it. I think, to be honest, how the GDPR is going to play out will depend on the next two years of implementation. How harsh are we going to be with the interpretation of those rules? We could decide to take strong interpretations of them, which would include significantly increasing the requirements vis-à-vis children and making sure they understand what they are doing. Continual, ongoing consent; repositories. One of the things that children said was, "I can't even find out where all the information about me is." There is no obligation for someone who holds

data about me to tell me they have it. There is a legal obligation to make sure it is up to date but they do not have to contact me about that. There are many mechanisms there where we, not just in the UK but generally across Europe, should be taking a much stricter interpretation of data protection law. The GDPR gives us this opportunity—two years to try to clean up our act and get a bit more responsibility into these businesses.

It absolutely applies to children. The companies that have the under-13 rule—which of course is not a UK law but US federal law; we do not have to have anything; the UK has not stipulated anything about age—know that kids under 13 are using the site and they are not doing anything about it. There is not even an attempt to do age verification. Much as we say it is difficult, the fact that they know, blatantly, that they have kids on there means they are not complying with the data protection law. All we need are a few serious court cases for that £2 billion or whatever—2% of maximum global revenues; it might wake some of them up.

Earl of Caithness: Given what you have said, do you think there is enough protection under the existing law, and is it just that the whole thing is so spread out that nobody has brought it all together, or there is no group that is bringing it all together? How does this affect 18 year-olds? I was thinking of the subject access request. Should a child have to pay £10 for that? Does that not put a child off, if they even knew about it?

Professor Derek McAuley: Indeed, and given how many people hold data about me, at £10 per subject access request, I would be bankrupt. Under GDPR—I might have to bring a legal colleague in here—I believe it is supposed to be online and free, to be able to ask at a reasonable frequency. Given that all of this content is digital these days, it is all ready to be made available if someone can authenticate themselves. In that sense, it should be free, so one of the things we might work on are the tools that would allow children to be able to access that and to understand what it means, and then to start to educate them about their digital footprint.

The Chairman: Our legal experts in the next session may help us with this one as well.

Q43 **Baroness Kidron:** You have segued into what I was interested in, which is this question about industry responsibility. I think it is palpable to us as we take evidence that people talk about schools' responsibility and parental responsibility, but when we try to get to the nub of what a parent or a school could do, the tools are not really available for them to make change. It seems that maybe industry has to help make change. I wonder whether each of you, from your own point of view, could say. You have mentioned things such as UK Verify—why does industry not do something around that?—and terms and conditions, in your report—why does industry not do something about that? I would really like to hear from you what industry could do that is a little bit more radical and a little bit more user-friendly when we are talking not simply about protection but about the normative use of “children being children” in this digital

sphere.

Professor Derek McAuley: Stop trying to monetise every piece of data. The assumption that there is a pot of gold at the end of the data rainbow drives industry at the moment. Many of the dreaded internet-of-things devices, in which the next generation of devices will have embedded technology—they may not even have a screen by which you can give consent—will be streaming data somewhere and people will be processing it. Internet Barbie dolls are already on the market. There is no point at which anyone is perceiving they are giving consent to having their audio or video streamed to the far side of the planet. This thing would stream my audio if I pressed the button to servers in America. That will be embedded in our world.

This is only because there is a belief that somehow after you have bought the product they will be able to monetise the data somehow, so they must grab all this data. It is irresponsible business models that are driving this. It is people thinking that, instead of just selling a product that has technology in it, they must sell a service and track you for all time. I think in industry there is this mind set which is driving everyone at the moment because they think that is what is making Google a lot of money. It is foolishness and in the long term will cause harm, in the sense that in the long term people will not adopt these products if they are constantly reporting on them. It is in industry's own long-term interest, which of course is one of the challenges industry has, that it does not tend to think long term. It would be better if they were much more attuned to the privacy issues and not sharing data when they do not need to. It could do a lot itself.

Mark Donkersley: We are clearly coming from a different angle on this, in that where we are receiving and where we are viewing behaviour, the digital environment is the vehicle; it is not the cause of the behaviour in the vast majority of instances.

I would say, going back to Chatroulette, that yes, there are examples—there is anecdotal evidence where we could see that an individual has inadvertently stepped into something and that environment has then led to harmful behaviour and risk, but in the main they are the vehicle as opposed to the actual instigator of the issue. It is very difficult for me to offer a panacea for a fix for the technology industry.

Baroness Kidron: Is it not the case that most of the big companies are very well aware of the sorts of markers you are talking about and of the lack of offering of the safe space that Professor McAuley talked about? Is it not true that most of them would have—what did you call it—depression indicators? They would have at scale, for billions of incidents, what you are doing in a very small way in schools; and rather than being monetised, that could be put to social use for the under-18s.

Mark Donkersley: Yes. I would say that they are not applying those markers to any degree. It is veneer-thin. There is no way that some of the Leviathans that Derek mentioned, with their population of users,

could handle all the material that would come back the other way if they had sensible markers in their system to identify risk and misuse, and so on and so forth. I think it is wrong to expect them to be able to do it. Yes, they could always do more than they currently do. As I say, we have evidence, experience, where we see some horrible situations. We have managed to alert somebody to intervene and protect, help and support an individual here, but there is probably something far worse that has happened at the other side of the world that nobody is able to trace.

The Chairman: I have to call matters to a halt as we have gone miles over time, but that is a sign that we have been absolutely absorbed by your evidence. We are extremely grateful. Thank you both very much indeed.

If you have views on the role of the education system, whether PSHE education should become a statutory subject, for example, please drop us a note. That is the outstanding area we were here to explore with you but everything else we have covered very fully indeed and we are very grateful to you. Thank you for coming.

Examination of witnesses

Adam Glass, Partner, Lewis Silkin Solicitors, and Steve Wood, Interim Deputy Commissioner, Information Commissioner's Office.

Q44 **The Chairman:** Welcome, Adam Glass and Steve Wood. Thank you very much for waiting patiently to join us. As you can tell, we were deeply embedded in the previous session but we are delighted to have you with us as our legal experts today. Thank you for joining us. I am going to ask you both to introduce yourselves. If you could do that and if from the Information Commissioner's perspective we could hear about your current role and whether that might be strengthened, you might just throw that in in your introductory remarks, and whether the ICO has a specific policy or approach regarding children, and children of different age groups indeed, that would be a helpful opener for us to get us cracking. Steve Wood, would you lead away with those themes in mind?

Steve Wood: Thank you very much, and thank you for the invitation to come and speak to you today. My role is deputy commissioner at the Information Commissioner's Office. We are the UK's independent regulator of the Data Protection Act and the Freedom of Information Act and another piece of legislation called the Privacy and Electronic Communications Regulations, which covers areas such as direct marketing.

Regarding the ICO's role focused on data protection, we have a range of powers and functions under the Data Protection Act. We can hear and adjudicate on complaints from members of the public; we have enforcement powers, so we can take action against organisations called

data controllers under the Data Protection Act—we can take enforcement action to force an organisation to stop using personal data, for example. We also have the power to fine data controllers under the Data Protection Act. We have had those powers since 2010. You may have seen the latest fine we issued in the media last week, which was the £400,000 against the internet service provider TalkTalk. We also have a role and a function in disseminating good practice to organisations. That is really about education and guidance.

We also have a role in promoting guidance and awareness—

The Chairman: Sadly, we need to interrupt you, and you have only just started. Profuse apologies; we need to vote on this amendment.

The Committee suspended for a Division in the House.

The Chairman: I was asking you about the ICO's policies and whether there was a particular approach regarding children, and indeed children of different age groups. Steve, I am afraid we cut you off in full flow on that theme.

Steve Wood: Thank you very much, Chair. Yes, I will continue. I gave a general overview of what the ICO does earlier but I will talk a bit more about our activities in the area of children, and particularly relating to the internet.

The first thing is I think increasingly, particularly over the last five years, the ICO has recognised the importance of the issues that have emerged, and has started to develop further strategies to look at the issue. The first area where we have done a considerable amount of work is in the area of education. Originally, going back over five years, the ICO had a specialist section on its website aimed at young people and children, which was not particularly well used. We took further advice from experts, which said that for the key messages the ICO had about children and young people becoming more aware of how to control and manage their own personal data, we were going to have to do more to embed this in teaching in schools. We invested a considerable amount of money in a project working with education consultants from the University of Edinburgh to develop a programme of developing teaching materials for primary and secondary schools, which we have promoted to teachers. We also responded to Department for Education consultations on the national curriculum to try to have these issues better embedded in the national curriculum.

The approach we have taken, and the reason we try to embed the information in the curriculum, was particularly trying to understand the difference between e-safety, which was starting to be taught more in schools, and the concept of individuals learning how to control and manage their personal data and feel empowered, which is a slightly more nuanced topic. We wanted to add something from that perspective, so we have continued that work and will continue to promote the use of those materials.

We are also aware of and interested in the possibilities of greater partnerships with organisations, as certainly the Data Protection Act and the ICO do not have all the solutions in this area. We have a relevant and useful role to play, so the more we can work with other regulators and develop partnerships, the more we can tackle that, which is another area.

On our approach to guidance to organisations about issues relating to children, we have not developed a lot of specific guidance, labelled as guidance, about processing personal data about children. We have more taken the approach to embed children's issues in lots of different pieces of guidance, so we have guidance about processing personal data in mobile applications; we published a new piece of guidance last Friday about privacy notices, which is obviously an important issue relating to transparency on the internet, and we had a section relating to children in that. We are very much focused in the guidance we are producing always to highlight to organisations the importance of the particular issues relating to children. Because the Data Protection Act does not have any particular reference to processing children's personal data, we developed what we called a risk-based approach in our guidance, which stresses the importance of organisations assessing for the type of processing they are doing, the types of uses of personal data and the types of personal data they are collecting, what types of safeguards they should put in place relating to that context to make sure they can understand the particular situation that they are processing the personal data in. In some situations that could include parental consent but we have not taken a blanket approach to that; we have taken a risk-based approach. I will leave it there.

The Chairman: Thank you very much. Please introduce yourself, if you would, and Lewis Silkin as well.

Adam Glass: My name is Adam Glass. I am a partner at the law firm Lewis Silkin. My area of expertise is media and IP litigation, so I have a lot of experience in representing clients who have problems, often online, whether that is defamation or misuse of private information or that kind of aspect. I have a lot of experience of the practicalities of trying to obtain remedies for them, and using social media platforms to obtain information from them on which to bring a cause of action or obtain a remedy for clients.

The Chairman: Thank you very much.

Lord Gilbert of Panteg: Can I pursue the discussion the Chairman started about how you view children and young people in different age groups, and in particular the balance between intrusion, which is necessary to protect them—schools have a duty to protect children but it is quite intrusive—and their rights to privacy, and whether that balance changes as children and young people get older?

Steve Wood: I am happy to answer that. The Data Protection Act has a number of principles embedded in it, including the concept of fairness and transparency, and also the concept of legitimate interest, which should

allow a school or an organisation which wants to use personal data in those situations to assess the type of data they are collecting and to make sure it is fair, transparent, and proportionate. Transparency might either need to go to the parent, depending on the age of the child, or to the child. The Data Protection Act has these principles, which we believe are flexible, which will allow an organisation to act in the best interests of a child in particular situations but also to consider the intrusion into privacy that might take place.

The Data Protection Act sets out a number of areas where organisations always have to focus on proportionality as the key principle, making sure they are only collecting the information they need. That is a duty on all organisations under the Data Protection Act.

Lord Gilbert of Panteg: You have no specific view or guidance as to how that balance changes for different age groups?

Steve Wood: We have not gone down the route of saying it changes at age 13. Our approach is to look at the particular situation. It may be in certain situations a child of 13 could understand what was being explained to them and it might be fair in that situation to provide some information for the child and for them to be able to interact with it. In other situations it might not be appropriate.

The stress and emphasis we want is to put it back on the organisation. There is not an easy slide rule to go to in guidance to say the child is age X, therefore you need to do X, Y and Z. The responsibility is on them to assess the particular context of what they are doing. The key tool we promote for this, which is not specifically focused on children, is a concept called a privacy impact assessment. If an organisation was doing something unusual or extensive with personal data, we would say they need to complete a privacy impact assessment, which has a series of questions to guide them through the right balancing exercise which perhaps you are alluding to. The General Data Protection Regulation, which will come into force possibly in 2018, will contain stronger provisions on data protection impact assessments, explicitly promoting them on the face of the law, which we think is a positive development.

Q45 **Lord Sheikh:** I want to ask you about the amount and volume of work you do on data collection and legal sharing of data. Are we doing enough? Should we increase it? If we were to increase it, what would the benefits be? The second part of my question relates to what the ICO told the Committee: "In reality there may be little that can be done to prevent unscrupulous third parties from harvesting a child's data and using it for inappropriate purposes." How can this situation be improved or mitigated, for example through making data collection more transparent and understandable for children?

Steve Wood: I will answer both of those questions in turn. The issues which often emerge around the benefits of increased data collection and data sharing will depend on different sectors and different uses of data. Certainly in the commercial internet sector, better use of personal data

can lead to better products for individuals. It can lead to more personalised services that individuals like using, and for a child that can mean that a cookie is set on the computer which means they can go back to carry on the game they are playing. Those are the sorts of benefits that can come from personalised services, which sometimes need unique identifiers or more information about individuals.

There are certainly benefits which can come from the use of data, particularly when it is aggregated for research purposes and social benefits in those areas. Where we would stand on all those issues as the ICO is making sure it goes back into that process I talked about earlier, still making sure the uses of the data are necessary and proportionate, and how they are balanced against the harms and the issues for the individuals. The heart of it must be that we need to do better on transparency, making sure people understand how the data is used in those situations.

Turning to your second question, about what can be done to prevent the harvesting of personal data of children, we made that statement to highlight the importance of getting things right first time. That goes back to the importance of transparency and better user controls for children and young people on the internet, because once a picture or a piece of information is publicly available on a website, as it stands, it is quite easy for that information to be harvested and re-used. Our emphasis is on much better prominent and clear controls for individuals, so it is only one click away or it is very accessible. Equally, it does not just have to be one notice on a website that does this. The document I referred to earlier that we launched last Friday, the new *Privacy notices code of practice*, has tried to get away from the concept of a big, monolithic document—we have all seen them; the statements about them being longer than “Hamlet”, et cetera—very much privacy information can be embedded and can pop up in lots of different places in a website to build someone’s knowledge as they understand what the service is doing with their information. Organisations have to redouble their efforts in transparency and better controls.

There probably also needs to be more innovation around technology. Is there more that can be done around standards and ways that data can degrade or automatically expire and can easily be re-used? We do not have all the answers to those questions at the ICO but under the new Information Commissioner, Elizabeth Denham, who took up post in July, we are in the process of establishing a more significant technology function at the ICO, and a grants and contribution programme; we would hope to actually fund innovation in this area to see if there are better privacy-by-design solutions, to try to work with industry to get that type of work developed.

Lord Sheikh: A very quick supplementary: how safe is your data? With all these people breaking into the data, how secure is your collection?

Steve Wood: It is a question which was obviously at the top of the news last week, when we issued that fine against TalkTalk. TalkTalk is a large

internet provider, but the attack on TalkTalk involved a technique which is relatively simple, because it was undertaken by some teenage hackers. Data can be secure; organisations can secure data completely or absolutely, but they must constantly redouble their efforts to secure the data. We are saying security and data protection should be a boardroom issue; it should be recognised at a high level of organisations so that the messages go down from the top.

Baroness Kidron: Can I just ask something very precise about what you are saying? The work you are doing around terms and conditions is fantastic but there is one fatal flaw: if you do not tick "Yes", it does not work. Not only in building up a profile but in little pieces and learning to say "Yes" to specific things, is there something you can do with industry that allows people to use services? Young people in particular have a real problem: if the service does not work unless they say "Yes", what kind of choice is that?

Steve Wood: I guess the point you are making is sometimes it is a take-it-or-leave-it approach.

Baroness Kidron: Almost always.

Steve Wood: We are aware of the pressure on young people to use certain types of services. We are interested in whether sometimes there should also be a granularity of consent. The case where we took action on that involved a public sector body. UCAS, the university admissions organisation, had a mechanism where third parties could direct-market to individuals on the UCAS database, and the consent for that was wrapped up with individuals wanting to receive the marketing and also information about careers and health. Perhaps the child would want the information about careers and health but not the marketing. In that situation we made them sign an undertaking to separate out the consent. I cannot say too much about it, but we are also investigating the current case involving WhatsApp and the sharing going from WhatsApp to Facebook in the new terms and conditions. That is pretty much a take-it-or-leave-it situation, with not a great deal of control about the data. That has triggered our interest.

Baroness Kidron: That is a policy issue, not a technological issue.

Steve Wood: Yes. The solution is in a range of areas. I would not say we have cracked all those problems but I was trying to say we are aware of it and we are trying to do more to promote that approach.

Baroness Benjamin: On the subject of personal data, at what age can someone be said to be able to understand an agreement they are making regarding their data and its usage, as well as other terms and conditions? What evidence is there to suggest that 13 is the appropriate age at which parental consent is not needed?

Steve Wood: It is a difficult question. The evidence for age 13, particularly in the online context, is mixed on how appropriate a very

broad cut-off date is. In the European data protection regulation which has been negotiated in Brussels over the last five years there was extensive debate about what the age should be in that legislation. In the end EU member states could not agree, and they put in the age of 16 but gave the member states the choice to decide to lower it to 13 if they wished. To have a broad, blanket provision in law which can link into a particular age indicated perhaps the lack of strong evidence. There probably is a need for more research to understand what the particular issues are online. Age is often quoted in other contexts, and perhaps learning could come from other sectors about where young people are consenting and that has become the rule of thumb.

Certainly the experience, and the evidence I am sure you have heard as well, is obviously that 11 and 12 is a crucial age, because it is when children start secondary school. In the year before they start secondary school there is a lot of pressure and a lot of interest in starting to use online services. The age issue probably needs to reflect the current circumstances, which is why we were quite cautious in our support for the age level set in the General Data Protection Regulation, because we were worried it was a broad cut-off and might give a false sense of security once that consent is given in that situation, because once the consent is given, in any case the young person is still using the service, and it is how the service protects them as well. It is only one solution in the whole situation.

We are supportive of a risk-based approach to using age verification in certain situations. It might be a blunt-edged tool if it is used very broadly, and will it have the intended effect?

Adam Glass: The answer to the question is it seems to be that somewhere between 13 and 18 is where people think a child or young person can understand an agreement. Obviously, generally UK law is that under 18 you cannot enter into a contract, with a couple of exceptions. In some ways it is arbitrary. I think 13 is probably very much following the lead from America and American legislation. A lot of social platforms are US-based and have legislation that says 13 or under in relation to data protection collection.

Obviously, the GDPR that may be coming in in a couple of years sets that arbitrariness at 16. I am not sure the ICO is being cautious, because member states cannot go lower than 13, so between 13 and 16. The ICO I think is plumping for 13, so the lowest age range. I am not sure if that is cautious. Basically, between 13 and 16 seems to be the fluidity. Of course, some children are more mature than others, some are more vulnerable than others. There is no science to this. I am sure there have been lots of social studies done by academics or whatever as to when and how, but I cannot see how anyone can positively say that you would definitely understand something at age 13, 14, 15 or 16. Obviously, someone has to take an informed decision, and it seems that between 13 and 16 in the next couple of years is where it will be.

Baroness Benjamin: Is there a role for parents to play here then?

Adam Glass: There is always a role for parents to play.

Baroness Benjamin: Some parents do not literally understand the rights and what their children are exposed to and what they are doing.

Adam Glass: I think that is absolutely right. I am not sure children and young people understand their rights—almost certainly not in relation to what their data may be used for. I am sure if you took a straw poll outside the school gate, most parents will certainly not have heard of the GDPR and probably do not know the rules around data protection in the sense that lawyers do, or people involved in using the Data Protection Act to further a means, for example a legal remedy. I am sure parents do not understand.

Baroness Benjamin: If children understood how their online material and data was being used, do you think they would be horrified? Should they be educated about this?

Adam Glass: Of course, and I think the education is going on, and even younger than the age when at the moment they can give consent. I have a daughter of nine and she is already interested and wants to explore the internet. She is not getting that opportunity yet from me but it is way younger than 13. The duty or obligation is of course across the remit of schools and parents. At my kid's school quite a lot is done: they have a lot of classes and whole-school discussions about online, the dangers of being online rather than necessarily how their data is being used; the dangers of chatting to people you do not know or may have only met once, and things like that. Absolutely, if we can educate parents more, it has to be a good thing. I am not sure how you can enforce that or make it better [as relates to parental involvement with their children].

Q46 **Baroness McIntosh of Hudnall:** From the point of view of legislation, or of us as legislators, there is quite a lot in the ICO evidence that you submitted to us, Mr Wood, where you stress that age verification, for example, is not an altogether useful tool, that it has drawbacks, and that anyway, as you put it, a resourceful child can almost invariably get round it. Why are we spending so much time arguing? It feels like an angels on a pinhead kind of argument whether it is 13 or 16 or 15 or something in between, because who is going to be in a position to enforce it? I am overstating that but is there an answer?

Steve Wood: The way I would answer is that it always has to be the responsibility of the organisation processing the personal data; they have the responsibility to assess the risk of the type and the nature of personal data that they are using.

Baroness McIntosh of Hudnall: But how are they to verify the source of that personal data or those personal details? If you say you are not competent to enter into an agreement to supply that data unless you are—fill in the blank—but you, the agent in this, the child, are perfectly capable of submitting a completely false prospectus to the internet provider, which will absolve them of any responsibility for not having

done their bit of it, what are we to do about this?

Steve Wood: To go back to the responsibility of the organisation, they have a responsibility to assess the risk in that situation, and, depending on the risk, they should put in place more robust solutions to verify the age and the identity of the individual and the parental consent. That is the approach taken by the Federal Trade Commission in the US. It is still not a perfect solution—you played the evidence back to us in that a resourceful child can sometimes get round it in these situations, which is why I think it is quite important to come back to the basics, that organisations should only be collecting the information they really need in that situation, because that reduces the risk as well. It will be a combination of factors which tackles this tricky problem you have rightly highlighted.

Adam Glass: I was just going to say something about the robustness of the process: if a child says “I want to go online”, “I want to receive some data” or whatever, and clicks, the process can be that they put in their parent’s email, that email is pinged to the parent, who can look at the privacy notice, et-cetera. With the better platforms, they will then go through, for example, a ghost payment on a credit card information, so the parent will get a phantom transaction, will have had to click on that, provide their credit card details, so they will know that their kid has given their information, wants to be set up on an account, and the parent will have gone through that whole system for that, and they will not be able to be registered until the parent clicks and says, “I have given my credit card and I can see it has gone through.” The better platforms do that well. That is one way of having good verification.

The other method of enforcement of course is lawyers occasionally holding people to task if they do not. There was a case last year, which has been settled, confidentially settled, against one of the social platforms, where a father brought a case on behalf of his vulnerable child, who was 11 at the time. The child had set up multiple accounts and was posting and receiving information from men, and posting inappropriate sexual pictures. He brought a case, and basically accused the platform, held them to a duty of care, and said, “This is a negligence case. You have a duty of care to my child. You should have ensured the verification process was tougher.” That did not go the whole way, but there is a way. Of course, we have better law sometimes by taking some cases and obtaining judgments, whether statutory or common law.

Baroness Benjamin: I was going to touch on the law. As there is currently no specific provision regarding children’s data in UK law, do you think there needs to be some sort of law and would it be workable in practice?

Adam Glass: I do not think we do. I think there is enough. We generally have good data protection laws, the Data Protection Act. The GDPR, as you have heard from various commentators, will specifically probably strengthen and clarify certain aspects of that, in relation to lawful processing, transparency, legible, plain English.

Baroness Benjamin: But does it focus on children?

Adam Glass: Yes, Articles 6(a), 12 and 17 specifically relate to and mention children, for example 12 being transparency and plain language. It specifically says “if aimed at children”, that needs to be intelligible, transparent, clear, but also plain and clear for them to understand. Article 17, the right to be forgotten, will again specifically relate to data that was processed when you were a child, even perhaps if you are now an adult, that should be able to be deleted, and for further onward dissemination to be stopped.

Baroness Benjamin: Is it working?

Adam Glass: The GDPR is not in yet, but what I am saying is there are those specific references to children in those Articles [to the legislation]. It will depend on member states how widely or narrowly they interpret the general framework, and of course, with guidance from the ICO as to where they think we should be heading.

Baroness Kidron: Just on that last point: however, we are leaving the European Union.

Moving swiftly on, you said something, Mr Glass, about companies responding more quickly to copyright issues because they carry financial penalties rather than questions of harmful behaviour. I am interested in your position on that. Do you feel strongly about that? You seemed to be suggesting the law was in place and maybe if there were financial penalties—

Adam Glass: My experience is, certainly in the past—and things have changed quite a lot over the last couple of years—that social media platforms were more worried about an IP complaint, so to take down a picture, for example, and that would come down pretty quickly if you could show you were the owner of the copyright. They did not seem as worried about defamation, bullying, harassment. As I say, I think the tide has gone the other way regarding bullying and harassment, partly because of the terribly sad cases that we see in the press of children taking their own lives because of online bullying, and the social platforms have changed their game and upped it in the way that they respond quite quickly to those kinds of issues now.

Defamation has always been a tricky one. I have some sympathy for the platforms, because they do not want to be the arbiter or the judge on the balancing act between freedom of expression and defamatory material. There is no doubt in the past they would keep that up and take off the IP stuff pretty quickly. Whether or not there should be tougher financial penalties—I am not sure that would make a lot of difference to the big players, for which it is a pinprick to be fined anything.

Q47 **Baroness Kidron:** In this area of enforcement, I was also going to ask about this personal family and household exemption that the ICO have taken exception to. I do not think we understand it 100%. Maybe you

could unpick the problem for us.

Steve Wood: There is an exemption in Section 36 of the Data Protection Act which essentially provides an exemption when an individual uses personal data for their own household, personal or family use. If individuals set up a group on the internet to share photographs after a holiday or to interact with each other in that situation, the Data Protection Act is essentially saying that those individuals are removed from any responsibility as being data controllers themselves, as individuals, under the Data Protection Act, so we cannot take action against them as the ICO if that use is for purely household, personal, family use.

It does not absolve the internet company hosting the photographs. The issues obviously come in particularly how they would react and must have the take-down systems, et cetera, to be able to take down the content quickly if an individual complained about a certain type of information that was posted.

The Data Protection Act in its construction is probably more focused on making organisations accountable rather than on an individual to individual situation, which is obviously a different step for a regulator such as the ICO to take when there are other legal remedies, prosecutions, et cetera, for defamation which can be taken in a certain situation. Members of the public understandably can be very confused, and will come to us in certain situations where they have had an upsetting experience online, and perhaps will complain about an individual to us. We are trying to improve the signposting of where individuals can go if we think we cannot help because of the way the Data Protection Act is constructed. We are not necessarily criticising the Data Protection Act, because it is a big step for a regulator to step into that individual's space, which is important for freedom of expression reasons. It is quite welcome that yesterday, for example, the CPS published new guidelines about prosecutions for hate-speech online in relation to social media. That gives us a better place to signpost to give people when they are in an upsetting and difficult situation and there may be a remedy available to them in another area of the law.

That is how that particular exemption works. We would probably more target our enforcement action against a data controller, to make sure they take their responsibility seriously, particularly if there were repeated or systemic problems, perhaps repeatedly not reacting to take-down requests from individuals in genuine situations where they should be looking and considering those carefully.

On the point about what we can do under the GDPR, where the step change is, at the highest level it is possible to fine 4% of global turnover, which is what is called a competition-level fine. It is more serious. We wanted to have that really big stick in the cupboard. It would be for the most serious cases and will probably be used rarely, but it does up the game in getting organisations to take it seriously, so more of our efforts

will always be focused on organisations rather than that individual to individual interaction, which is exempted under the Data Protection Act.

Baroness Kidron: Very briefly, I would like to ask this, as so many young people complain about non-response. They do not understand how they can work out their takeaway is two minutes, one minute, 30 seconds, at the front door, but when they make a complaint they find it very difficult to know whether it has been opened, responded to, what the status is, and so on. I wonder whether you think that the culture, and the law or regulation, are in the right place regarding complaints.

Steve Wood: I think organisations have to continue to up their game in that area. If the number of complaints increases, they have to think about the reasons why that is happening. In the situation you described, that quite a few years ago perhaps they were more responsive to copyright infringements probably was true. As Adam said, I would agree it is improving, there is a better prominence and availability of those services.

Also, the individual should be able to do it themselves; self-service is the best option; to easily press a button to delete or remove your data in a clearly useable service is probably the best situation. The position can improve.

We also have better case law now. We had the Google Spain judgment a few years ago about the so-called right to be forgotten, which enabled individuals in that situation to request that search results against their name be removed from Google. Initially Google resisted that, and were not interested in that type of area, given how that would interact with their business model. Once the judgment came in, they had to comply with it, and in fairness to them, they have invested in improving that service. Google are also fairly transparent. They have published quite a lot of data about when the take-down requests are coming, and they are removing things such as social media results from search engine results. Lots of those cases are probably young people who did something embarrassing when they were 14, are now applying for university and they want that information removed from the search engine result. It is a step in the right direction that the case law is helping in that situation.

Q48 **Lord Sherbourne of Didsbury:** A very simple question: in your evidence, talking about taking down content, you said, "Perhaps service providers should be encouraged – or required – to do more to clean up problematic content from their networks." Just give me one or two specific ideas that you have in mind for what you would like them to be required to do.

Steve Wood: I think it comes down to when they need to be proactive and when they should be monitoring the information they hold, to understand that information, particularly—it goes back to the answer I gave before—about when an individual has information that they want to have forgotten. The organisations which hold that information should be responsive to that request.

Lord Sherbourne of Didsbury: When you say they should be required, do you mean by legislation? How would you require them to do it?

Steve Wood: With the legislation, if the GDPR comes in, to some extent, Article 17 of the GDPR will give the right to be forgotten, which is the right to request to have information deleted. There is the possibility that that will come in and that will provide some of that remedy. Some of it may come down as well not just to legislation but making sure that particularly the major providers all understand the good practice of having a very responsive system to take-down requests.

Lord Sherbourne of Didsbury: How would you make sure they did?

Steve Wood: There are different ways we can do it. We could do things such as proactive audits, where we can go and look at how the different providers are responding. We did what we call an international sweep a few years ago, working with other international data protection authorities. We went and looked at the websites of different organisations providing services to children online, and we then publicised the findings. So there are different ways we can do it.

Lord Sherbourne of Didsbury: That is encouragement really.

Steve Wood: Yes. Probably a mixture of hard and soft measures will be needed.

Baroness Quin: I have a question but I just wanted to pick up on something else. You referred on a number of occasions to the right to be forgotten. I may be wrong in this but I had a feeling that the Government's view was not very much in favour of the right to be forgotten. From what you have said, you sound more favourable towards it. Can you explain what the current thinking is about this?

Steve Wood: Yes. We are an independent regulator, so our view can be different from the Government's view. I gave evidence to this House after the Google Spain judgment in 2014, so I am quite aware of what the issues are. When the judgment first came out, the term "right to be forgotten" was quite emotive; people thought it was about censorship, deleting information; quite strong analogies were used about taking books out of libraries, when actually, if you look at the judgment, it is a more proportionate measure. It is about the right of the individual to have search results which are returned against their name—so you type in someone's name, a certain link appears in that search result, the individual makes the case as to why that search result should not appear against their name. It does not remove the information completely from the internet in that situation, but it was about removing it from Google in that situation, because that can be one of the most personally intrusive things, as the way you look up someone when you first meet them is you put their name into the search engine. It is quite a proportionate step in starting to give an individual some more control over their data.

They could also go to individual websites and ask individual websites to remove the information. It was portrayed quite negatively in the media I think because they saw it as censorship. The reality is that it is a proportionate tool for individuals to control their information. Equally, it is not a magic bullet in solving quite a difficult problem; if you have a mass of information about you on the internet, it is very difficult to get it removed.

Q49 **Baroness Quin:** That is very helpful. Thank you. I was also going to ask, and you have touched on it in answers particularly to Baroness Kidron earlier, regarding industry: is there more that the industry could do to make their data collection practices and other terms and conditions clearer and more understandable for children? I know you touched on this before but have you any further thoughts about it, in particular how companies could be either (a) encouraged or (b) required to adopt such measures?

Steve Wood: I will try not to repeat the answer I gave before. We would say there is more industry can do. Again, to reference the forthcoming GDPR, there is a stronger provision in that for codes of practice, and they specifically say that codes of practice could be drawn up relevant to children's issues. To have some stronger codes of practice for industry might be one way of addressing it, which is a tool we could develop in this country, or industry-wide across Europe, to look at the particular challenges.

I would say it is always the mix of the regulatory tools we will use. We will take on and look at and investigate the worst abuses, and those might be enforcement cases or investigations to make an example of the worst cases. We need to improve the guidance to make sure organisations are getting the basics right. Industry needs to do more of its own codes of practice, to be constantly raising the bar. We want it to be a competitive advantage of a company to sell themselves on their privacy practices. It is starting to happen but it is still probably in its infancy. Why should it not be the case when someone is looking at two competing services that they could think "I want to use that one because it is more privacy-friendly"? In an area with a lot of market domination, and obviously market domination is not our responsibility, that is where the challenge lies.

Earl of Caithness: Does it make any difference to your work whether we are in or out of Europe, and, if we are going to be out, do we need to bother to enforce GDPR?

Steve Wood: This is obviously a question for the Government to decide. We are the regulator and not responsible for what the rules should be. Our view as a data protection regulator would be that the case for a strong, effective, progressive data protection law, whether that is a UK law or a European law, is strong because the challenges of the digital economy and all of the issues we have been talking about today remain the same whether we are in Europe or out of Europe. We will always make the case to Government to make sure we have a strong data

protection law, with the right building blocks in place. Lots of those building blocks are in the GDPR, which could come into force in 2018, before we leave the EU in any case.

Businesses are telling us they want guidance, because they do not like the uncertainty. They obviously want to start preparing for the new law, and if that is going to include age verification, obviously it is important for them to invest and plan ahead. That is the feedback from businesses. Multinational businesses operating across Europe in any case will want to think about complying with the GDPR because of their European operations as well. It is still a relatively early stage of these issues being discussed about the future of data protection. That is as helpful as I can be.

Q50 Baroness McIntosh of Hudnall: The related question, which I hope you will be able to enlighten us about, is this upcoming issue of net neutrality in relation to European law, which we may or may not, presumably, be obliged to conform to, depending on what happens over the next couple of years. Can you give us some sense of what impact, if we are going to be in the position of implementing the net neutrality rules, that will have on the arrangements the Government already has with ISPs?

Steve Wood: The issue of net neutrality is actually the responsibility of Ofcom. I am cautious about saying very much about that matter because it is not our regulatory responsibility.

Baroness McIntosh of Hudnall: Does either of you have a view? Given that there has been quite a lot of work done, as I understand it, to try to go for an opting in rather than other kinds of arrangements with ISPs, if this were to come in, would it be likely to undermine some of the protocols that we have begun to build up already?

Adam Glass: In what I have read about it, I have not seen anything that would mean it would affect the current protections we might have in relation to this area, but I have to say the pros and cons of net neutrality is a trillion dollar question. I have not quite reached the bottom of what it might all mean.

Baroness McIntosh of Hudnall: And you may never have to.

Adam Glass: Quite. It was recently voted down with the amendments at the European Parliament. Who knows what may or may not now be implemented?

Baroness McIntosh of Hudnall: The recommendation would be to ask Ofcom, would it?

Steve Wood: Yes. There are some parallels between areas such as the importance of transparency, for example, so we will discuss that with Ofcom in trying to make sure we give consistent messages if net neutrality does come in between transparency and the data protection rules and transparency in relation to net neutrality, to make sure these things are reasonably well aligned. That is about as much as I can say.

Q51 The Chairman: You may have some final thoughts for us, including any comments on the guidance from the Director of Public Prosecutions that we have been hearing about recently. Please share any final thoughts with us before we break. Adam possibly first.

Adam Glass: From the practitioner's point of view, my frustration when representing clients has been that certainly the civil or criminal route each has its own value. Generally, with the civil route, where, for example, you might have the most success in trying to get something removed straight away from the internet—if there is an emergency you can get an ex parte injunction, for example—whereas with a criminal matter you are in the hands of the state and the investigation, and you may get no interim order from a judge to get anything removed, and he does not have that power effectively. Often I am looking at the civil route, and the difficulties are often that you are going to multiple people—it might be a mobile phone company, it might be an email provider like gmail or Yahoo—trying to get information because I want disclosure of someone who is hiding behind an anonymous IP address. To try to get to the bottom of that can often take multiple attendances on a Master in the Queen's Bench Division to get an order that I then have to serve on the various people to get the information. That will often have to go to the US, because that is where the servers are placed. The difficulties in getting to somewhere where I can actually serve a letter, to find the person that I want, can be time-consuming and very costly for a client.

Certainly in the past the platforms have been difficult, where they have said, "Well, we are not based in the UK, we are based in the US. You have to serve on us in the US..." I can get any order from the UK, and generally judges are very supportive when we need to get that, but I would then have to serve it in the US or other jurisdictions, and certainly outside the EU that can be very difficult. Particularly in the US they have various principles, free speech being just one, where they do not necessarily even want to take notice of a UK order and have it enforced. To do that you would have to go through the state system, et-cetera. Those for me are very practical issues, and you can rack up quite a lot of money before you even have somewhere to serve a letter of complaint on someone.

Baroness Kidron: Can I just say for the record you have to not only have an active parent for that but a rich, active parent, since we are talking about children.

Adam Glass: Absolutely. Absolutely right. Lots of law firms take matters pro bono or reduce fees to try and help but you can easily rack up thousands of pounds before you even obtain the information by which you can start your claim. That for me is one of the downsides of the civil route, as I say, as against the criminal one, where at least you have the state bearing the costs of the investigation, but you might have a year before you come to trial and the stuff remains on line; you will not get a judge taking it off in a criminal case, and maybe someone goes to prison

or is fined, but the stuff can still remain online. It is up to the platforms to take it off.

I would like to see a cheaper, more effective and more expeditious route to obtaining information that can enable lawyers to assist young people, children, and their parents to take speedy action. The cost is a big barrier to that.

The Chairman: Steve, any final words?

Steve Wood: I think just to echo the comments I have already made about there probably being a range of solutions, going from the education and transparency points I made earlier down to the legal points and what we may be able to benefit from if the GDPR comes in and also the mechanisms we can have to enforce, so it will be a range of solutions that help tackle this difficult area.

The other point I had to make in my final comments was similar to Adam's, which is the international dimension to this, which makes it a lot more challenging. This is why it is probably important as well that we are going to have to have a move towards global standards on this, because it will be the way to make it easier to operate for the average citizen in the situations that Adam talked about. At the ICO we have led in the development of a global enforcement network for data protection regulators around the world, which enables us to share information or pass on concerns when a member of the public comes to us in the UK, complaining about a firm which is solely established in the US but perhaps offering services to UK citizens.

One example of that is the case of a company called VTech, a child's toy manufacturer which makes smart tablets and screen-based toys for quite small children. They had a really large data breach, and earlier this year we were able to liaise with the Hong Kong Commissioner at least to try to get some information and answers to be able to feed back to people in the UK and parents who were concerned about this. Ultimately, the solutions have to be global and we need a strategy to really make it work so people do not have to have recourse to a lawyer. It should be possible for a regulator such as the ICO to act on behalf of the public. Even though we cannot take every case forward, we should at least be able to interact in the most serious issues on a global scale.

The Chairman: Thank you both very much indeed. We have had a long afternoon. We are very grateful to you for staying with it. It was all good stuff. Thank you very much indeed for joining us.