

Digital, Culture, Media and Sport Committee

Oral evidence: Connected tech: smart or sinister? HC 157

Tuesday 17 January 2023

Ordered by the House of Commons to be published on 17 January 2023.

Watch the meeting

Members present: Damian Green (in the Chair); Kevin Brennan; Steve Brine; Clive Efford; Dr Rupa Huq; Simon Jupp.

In the absence of the Chair, Damian Green was called to the Chair.

Questions 279 - 369

Witnesses

I: John Edwards, Information Commissioner; and Stephen Almond, Director of Technology and Innovation, Information Commissioner's Office.

II: David Kleidermacher, Vice-President of Engineering for Android and Made-by-Google Security and Privacy, Google; and Leila Rouhi, Amazon Alexa Vice-President of Trust and Privacy, Amazon.

Examination of Witnesses

Witnesses: John Edwards and Stephen Almond.

Q279 **Chair:** Welcome, everybody. This is a meeting of the Digital, Culture, Media and Sport Select Committee. It is part of our inquiry into connected tech and for our first panel today I am delighted to welcome back John Edwards, the Information Commissioner, who survived the grilling of the pre-appointment hearing by this Committee, and Stephen Almond, who is director of Technology and Innovation at the Information Commissioner's Office.

Welcome both. For this part of the session, we are interested in data protection and your attitude to it. We have heard throughout the inquiry that connected devices collect significant amounts of data and operate without human input. Does this give rise inherently to privacy risks? Is it inherent in the design of connected tech that we have a new set of problems?

John Edwards: Yes, I think we do. First, thank you for the invitation to address you and it is great to be here in person, rather than beaming in from the other side of the world at an unsociable hour. I am happy to assist.

One of the key challenges with connected tech in relation to data protection is the lack of a user interface with the media. Some of these are just sensors that are collecting and transmitting data about the user with no real ability for the user to meaningfully interact with it. That does present a number of challenges.

One of the other challenges is the volume of data that is collected. They can be on all the time, constantly transmitting. That poses a challenge to one of the most fundamental, underlying principles for data protection, which is data minimisation. We have difficulty achieving in some circumstances the transparency that is essential to people enjoying their privacy and data protection rights, and some other challenges in relation to accessing information, knowing who is the controller in a complex data ecosystem, for example. Effecting their right to erasure or deletion is a challenge.

It is difficult to speak about the whole world of connected devices, but I think you are right to identify some specific data protection challenges that some of these devices present.

Q280 **Chair:** Do you think that tech companies suffer from an inherent lack of trust among consumers? Do you detect that people are worried about this next generation of things, where, as you say it is inert? You do not know, there is no obvious data control, all those problems. Do you think there is an underlying lack of trust?

John Edwards: The activity in the market would suggest the opposite. People are flocking to these devices. They are installing them in their



HOUSE OF COMMONS

homes. I think Stephen said six out of 10 homes has a connected TV now. We do not have good information to understand the trust relationship, whether this enthusiasm for these devices is based on an ignorance of the data issues that they represent or, conversely, whether it is based on an expectation among consumers that organisations such as mine are there to watch their back and to ensure that data protection standards that they enjoy in other aspects of public life are also applied to these devices and the data that they collect and transmit.

Q281 Chair: The question that will show how much we should be concerned, and this is a question to each of you, is do you have connected devices in your home?

John Edwards: I do, yes.

Stephen Almond: Yes.

Q282 Chair: Smart speakers?

Stephen Almond: I have a variety of devices, including smart speakers, but for me as Director of Technology and Innovation I feel it is important to engage with the market and to understand what is going on, and live the life of the consumers around the UK in terms of their experience of technology. I do tend to be eagle-eyed when it comes to the privacy policy.

John Edwards: I have a couple of smart speakers; I have a smart TV. I think the one thing that we ought not to lose sight of is that these devices can bring great benefits of convenience. For disabled people, for example, there are great benefits in being able to activate devices or access information by voice command, rather than manipulating a visual interface. There are advantages in having notifications of states that may not be readily apparent to somebody who is disabled.

I asked Stephen's team to compile a frivolous list of needlessly connected devices and he came up with quite an interesting one. There is a cat litter box that will let you know when it has been used, and we might call that a frivolous device and it is easy to mock. Just because something can be connected to the internet it does not mean it has to be, right? But of course I think Stephen quite rightly cautioned me to say, "Don't mock these things lightly", because there can be real benefits for the disabled community. Getting a haptic notification or an oral notification can be of value, to prevent that litterbox stacking up—I do not know.

Q283 Chair: I absolutely take the point, particularly about people with disabilities, people who are bedbound, things like that, that these kinds of devices can be very useful. Is it your underlying point that they will intrude on our privacy, but we just have to lump that for the benefits that they give?

John Edwards: No, I do not think so. With respect, Chair, I do not think they necessarily have to intrude on our privacy. Recognising that to



deliver what they promise requires a transmission and a use of data does not necessarily mean that there is an intrusion on our privacy, as long as that occurs within the expected foreseeable bounds.

I do think one of the risks is when the data is repurposed in ways that the consumer did not expect when they installed the device in question. To return briefly to your question about the levels of trust in society, in preparation for this appearance we did interrogate our own data sets to see whether these are matters that feature in our inquiries or in our complaints statistics, and they just do not. So again, we do not have good data to know if that absence is a result of ignorance of some harms that are being caused, or an acceptance that there is a transaction that is involved in purchasing and installing one of these devices and that people are willingly entering into those. If people are willingly entering into those, it is difficult to characterise that as an intrusion into privacy.

I do think that the risks that have provoked the Committee to begin this inquiry are real and are contingent. It is right that we are alive to these possibilities and that as a regulator we are working with industry to ensure that the risks are mitigated and that consumers get what is written on the box and do not get unpleasantly surprised.

Q284 Chair: It is an interesting point that people do not complain and do not appear to be worried about that. Is there any research done into the levels of knowledge that the population have about what information they are giving through these connected devices and if there are any worries out there? Stephen, maybe.

Stephen Almond: We have very recently funded some research through Cambridge University, through the beautifully entitled Internet of Stings project that they have been running, which did look at this and highlighted many of the concerns that John has outlined. It raised concerns around transparency and meaningful control and users' ability and understanding of the technology to be able to engage meaningfully with it, but also these concerns about the volume of data that is being processed. Is that what is necessary and proportionate for the purpose and the potential for repurposing of data? I know that as a Committee you have already explored the concerns around security and how people are protected from that angle.

Q285 Dr Rupa Huq: I want to ask a bit about the now paused data reform Bill that was put on ice in September to allow the new Ministers to get their heads around it. John Edwards, at your pre-appointment hearing to this Committee you said that the UK can "go your own way" regarding data protection while ensuring ongoing advocacy with the EU. Was that tapping into the zeitgeist and it sounded good at the time? Does what we know of this data reform Bill deliver this?

John Edwards: I will caveat my comment with saying that as far as I am aware there is nothing in the proposed law reform that would have a material effect on the ICO's ability to work in the space of connected



HOUSE OF COMMONS

devices. For the purposes of this inquiry, I do not know that there is much that I can illuminate. I think you are asking me to go beyond the inquiry, and that is understandable with this being my first appearance before Committee, so I will answer the question despite its lack of direct connection to the topic of connected devices.

I have been very pleased to be engaged with Government in looking at their reforms and from the outset my position was that I would like to see these reforms get to a position where I am in a position at the ICO to publicly support them. That means ensuring that none of the proposals reduce the rights of people in the United Kingdom; that the proposals do not put in peril the adequacy determination with the EU, and that the reforms allow me as regulator to make compliance easier and to reduce the cost of compliance for businesses in the UK.

I am happy that the Bill as introduced last year that now sits in Parliament meets those criteria and I have been happy to support it. The new Secretary of State did indicate a desire to engage with industry to see what other reforms might be warranted, and I think that the Government are still in the midst of that process, and we will again provide candid advice and our best expert input into that process.

Q286 Dr Rupa Huq: The Bill replaces the current regime with alternative arrangements such as senior responsible individuals with broad responsibilities. How will this differ from existing data protection officers?

John Edwards: From the position of a regulator, I will be assessing any non-compliance that causes harm and assessing penalties that are commensurate with the conduct of the organisation. An organisation that has invested in expertise to ensure that it meets its obligations can demonstrate mitigating factors if there is an incident that causes a problem under the law. I do not think the title, whether it is a data protection officer or a senior individual, is particularly material to that and my expectations of organisations will remain the same, given the nature of the process and the nature of the data that is being processed and the potential impact on individuals. That is where I set my standards.

Q287 Dr Rupa Huq: Depending on where you stand, simplifying things, watering them down, or making them more burdensome, do either of you have thoughts on this? Independent of what it says, how have key stakeholders responded to the decision to pause the Bill's progress and just what do you two personally think? Do you welcome this decision?

John Edwards: It is difficult for me to answer that question, but I would be happy to come to speak to the Committee about the Bill when it is before the Committee and answer any questions. It is your Committee. I am here giving you as much time as you have allocated, but I do think that if we go down the pathway of examining the Bill it does intrude into the time that you have set aside for this important inquiry. I will leave that to the Chair to determine the proceedings and the nature of the input you would like from my office.



Chair: We will see where we come to. Let us just stick to connected tech for the purposes of this hearing.

Q288 **Dr Rupa Huq:** On connected tech you have previously told us about the difficulties of engaging with these different players, the tech giants, because you are a national regulator, and their remit goes much wider. How have you tackled this challenge since taking post?

John Edwards: I will hand over to Stephen, because he administers much of what we describe as our upstream regulation, which means working alongside these innovators and these large transnational organisations to ensure that they are aware of their obligations in the UK. For example, we have established a sandbox where we will work alongside innovators to ensure that their products and offerings into the UK market are compliant. We have our innovation hub. Stephen could pick up from here and describe how some of those engagements provide assurance of compliance.

Stephen Almond: Going to the point that John has described, they are one and we are many in terms of the data protection authorities, but part of our approach must be about co-operation with other international authorities, be they within our own sphere or adjacent to our sphere in terms of other digital regulators. We do enjoy very strong, co-operative relationships with other privacy and data protection authorities around the world and we have practical information sharing arrangements, for example, with our partners in the US and other key jurisdictions where these firms reside, to be able to exert the degree of influence that you would expect.

In relation to the firms that present the highest risk and have the greatest reach across the economy, we maintain direct one-to-one relationships with these firms to ensure that we have advance awareness of key developments that may have significant impacts on the rights and freedoms of people in the UK, to be able to exert influence in the interests of UK plc at the right opportunity. We do offer, as John has said, a range of services for firms big and small to engage with us in goodwill on the application of data protection law to their new ideas. We have a regulatory sandbox where organisations can work with us to test their ideas and get an understanding of what our data protection concerns might be.

We have an innovation hub that has partnered with, for example, the Connected Places Catapult to support innovations in a variety of areas of connected tech, and later this year we will also be offering an innovation advice service for firms that want to consult us.

We are trying to do everything we can to help organisations get it right, but also to make sure that they understand their obligations in this area and be ready to act if they do not take them seriously.

Q289 **Dr Rupa Huq:** John Edwards, you previously said that there was



HOUSE OF COMMONS

potential for the UK to be caught between the US and the EU on data protection. Has that antagonism been borne out?

John Edwards: No, I do not believe so. I am not sure that I would categorise it as the UK being caught between. I think that there are opportunities for the UK to have an approach to data protection that is not exclusively European, and which engages with some of the approaches in the US.

I would return to the previous question and add to what Stephen has told you about some of our international engagement. A number of regulator network groups, for example, come together to identify common issues and there is a telecommunications working group which is a subgroup of the Global Privacy Assembly, which is where all privacy commissioners, information commissioners and data protection authorities convene. That group produces papers and position papers and recommendations on issues such as smart cities and connected autonomous vehicles, because we recognise the issues are arising in all the jurisdictions in broadly similar regulatory frameworks, and we set out our stall. I think it is very useful for the firms that are producing those technologies to see where we stand.

Q290 **Dr Rupa Huq:** Does the dearth of UK manufacturers, let alone European ones, when all the big players are Korean, Taiwanese or Chinese, make it difficult for policymakers here to set minimum standards on data, cybersecurity and so on?

John Edwards: It does present challenges. You are quite right to identify that. If you had asked me a year ago if there was a regulatory lacuna in terms of data protection, I would have said that there is a disjunction between the organisations that are providing the hardware, which is the mechanism for the collection of the data, and those that are deploying those products within the UK, and that it is very difficult for a data protection authority to regulate an organisation, a firm, which is providing the means to collect data but is not itself collecting data.

I think that the Government's response to that issue with the Product Security and Telecommunications Infrastructure Act significantly closes that gap. What that legislation will do is ensure that rules are promulgated, which means that a manufacturer, or an importer, would have to meet certain standards, and that includes in relation to security. So whether a connected device loaded with sensors is produced in the UK or is produced in China or Taiwan for import to the UK, the importer must certify that it meets those standards. I think that does go some way to address the important point that you have raised.

Q291 **Chair:** To follow up on one thing, you said that you make your hub and the sandbox available to companies big and small. Do the big companies play ball with that? Do they get involved?

Stephen Almond: Frequently not. It tends to be the smaller players who engage with us through that. That said, the new proposal we have that



we will be rolling out later this year of this innovation advice service has attracted interest from firms big and small. Because data protection legislation is principles-based, there are often lots of questions about how to apply that to specific technological contexts, and so the creation of a service that will enable people to say, "I plan on doing X. How would you treat this in terms of your interpretation of this principle?" so on is a crucial way of providing organisations big and small with regulatory certainty. We are seeing a likelihood of quite significant take-up around that.

Q292 Chair: Is your organisation big enough to engage the attention of people such as Google and Amazon? I have had personal experience in the past where I felt that Google were not listening because they thought they were big and the British Government did not matter. Do you ever get that sense from them?

Stephen Almond: I would say not. I would say that in terms of both the regulatory armoury that we have within the UK in terms of our law, but also the ICO's skill and resources, we command reasonable respect from the variety of tech firms. I would say it is a mixed bag. There are some that will proactively engage ahead of product launch, explain the privacy implications, and walk us through. There are others who we must remind occasionally that if they want to enjoy access to the ICO to talk through their products then they must give us fair warning and engage with us appropriately.

Q293 Chair: Who are the ones who are most difficult?

Stephen Almond: It is a spectrum. To be fair to the different firms, it quite often varies from issue-to-issue or period-to-period. It is a bit of a horses for courses question.

John Edwards: It is true to say that the kinds of companies that we are referring to here have enormous resources to invest in their research and development and their legal and compliance functions. When they are about to issue a product, they will do so quite confident that they are meeting regulatory requirements within the jurisdiction. We may differ in how they go about that, but usually they will come along to us not to seek our advice or input but to simply tell us what they are going to do. Would that be correct, Stephen?

Stephen Almond: By and large, yes. There are some cases where we have successfully achieved a degree of prior influence, notably through our collaboration with the Competition and Markets Authority to scrutinise Google's plans to phase out third-party cookies, where they are now working quite closely with us in advance of rolling out changes, to ensure that they are in line with expectations.

John Edwards: While some of those companies do present very real regulatory challenges, it is also important to note that they are very much alive to the implications of some of this technology and they will



select not to pursue market opportunities where they believe that there are regulatory risks. One interesting example was Google not proceeding with its Glass product. Now, I do not have insight as to whether that was in response to regulatory risk or public sentiment, but there were obviously significant implications in relation to that product from a data protection point of view and they decided after a very significant investment not to proceed with it to market.

Q294 Kevin Brennan: I think I would summarise that last exchange as from time to time they are all as bad as each other, but they will not do something bad if they think they will get caught. Is that a fair assessment of what you just said?

Stephen Almond: I think each of the firms has a different risk appetite. In relation to privacy you can see that some firms at least in their marketing will profess that privacy is very core to their values, and some will align themselves around other objectives that people may have. It genuinely is a bit mixed.

Q295 Kevin Brennan: I will leave that part there. Can I ask about your age-appropriate design code, which obviously is intended to regulate how data protection should apply to children and includes connected tech devices, such as connected toys and so on? If I were a parent of young children, which I am no longer, what sorts of messages would you like to give to me in relation to this kind of technology and my children's safety?

John Edwards: The age-appropriate design code is seen internationally as groundbreaking in terms of setting expectations and standards for children's digital online experiences. The concession to connected devices is to require that some of the standards that are there to protect children's online experience when they interact on the internet are also applied to those devices so, for example, things such as location tracking switched off by default and other default settings, which are expected for children.

Stephen Almond: Another area that we would consider is in relation to transparency. As John has already mentioned, connected devices may struggle to provide appropriate transparency, because they lack screens.

Q296 Kevin Brennan: Is it more difficult by the very nature of the devices to enforce the code or to be able to see what is going on?

Stephen Almond: In relation to the difficulty first with complying with the requirements here, it is inherently going to be more challenging to think through what is, for example, the right privacy information that should be provided that is suited to a child, if we are talking about transparency, and then how do you do that in the context of a connected toy where there may not be a user interface, where there may not be a clear way for the child to receive that information in an appropriate way? We know that several organisations are starting to think that through and to grapple with it.



In terms of our prioritisation—

Q297 **Kevin Brennan:** Before you go on to that, do you take any kind of proactive approach before products come to market, or is it a reactive approach to it?

John Edwards: We do not really have access to the product's launch time horizon, so we do not know what is coming down the pipeline—what is going to be in Hamleys next Christmas—and whether we should be in there. We do not have capacity to get ahead of that, but we are available to provide the sorts of services that we described earlier with the sandbox and the innovation advice, if those companies choose to engage us.

Stephen Almond: I would simply also note that in respect of our areas of focus for the children's code right now our priority is in scrutiny of things such as gaming, video and music streaming and social media in terms of the sorts of areas where we are seeing the areas of greatest concern. Connected toys is an area that we would like to be able to turn to in future, but in terms of the areas where we are getting the greatest volume of questions coming through and of interest are the ones that have been prioritised in relation to the children's code.

Q298 **Kevin Brennan:** The Oxford Internet Institute told the Committee that connected tech in schools has been used for mass collection of children's data and often designed without any input from teachers or parents. Does that imply any kind of failure on the part of the code and its implementation in this environment where you are most likely to find children, in a place of education?

John Edwards: I do not think so. We do not see any evidence of harm appearing through education technology.

Q299 **Kevin Brennan:** Would it concern you if there was a mass harvesting going on of children's data?

John Edwards: It is hard to know what that means. If schools avail themselves of Google Docs and Microsoft 365—any kind of tech tool that is available for use in the classroom can be characterised as edtech, and that does not mean that there are unique threats to children through the use of those tools, or the mass harvesting of identifiable information about those student learners or users. We are open to reviewing any product that is deceptive in the way that it is describing its data flows or is repurposing data in ways that are unexpected by students, schools or teachers.

Stephen Almond: Of course not all edtech is connected tech, and not all edtech would fall within the scope and remit of the children's code in terms of what it applies to. In respect of this inquiry, the focus on the use of connected tech in schools would be a narrower application.

Q300 **Kevin Brennan:** I know we are not getting into the future data reform



Bill, but there are some concerns, and it does relate to the age-appropriate design code and the 15 standards that are set out in that. Do you have any concerns that legislation of that kind could undermine the code if companies do not need to take data impact assessments or if they keep cookies as opted by default? Would that undermine the purposes of the code if future Government reform in this area were to go down that road?

John Edwards: I cannot see how it would because those standards are objectively assessable. Whether they have done a data protection impact assessment or what their cookie policy is, we are still able to assess the product that they are offering that is likely to be accessed by children and to determine whether it conforms to the standards required in the code.

Q301 **Kevin Brennan:** Would legislation possibly override the code as a statutory code if there was new legislation?

John Edwards: I do not believe that the example you have given would override the code. The code is a stand-alone set of standards and obligations. I am not aware of anything in the proposed reform that would come into conflict with those standards and obligations.

Stephen Almond: The code will naturally have to be re-laid so that it is in line with the new legislation and will have to be adapted in line with that. Those points in terms of what the code is aiming to achieve, the outcomes around it, remain fixed. Considerations for example of whether profiling should be allowed for children will still remain considerations in terms of the outcomes that we want to achieve, irrespective of the detailed rules around opting in and out of cookies.

Kevin Brennan: If you do cogitate further on that or have any other thoughts, do let us know in writing.

Q302 **Simon Jupp:** Good afternoon to you both. Connected devices, smart devices, whatever you want to call them, have many benefits, but we have also heard and seen evidence of some of the pitfalls, dangers and downfalls of them, one of them being that they can be used by perpetrators of domestic abuse in various ways—remote control, the automation of tasks, heating, lighting and also changing their material environment, which this technology can do. Is this something you are cognisant of? How much of an issue do you perceive it to be?

John Edwards: Thank you for the question. It is sobering to think of the range of ways domestic abusers deploy to maintain control over their target, and it is terrible to think of these devices being used to imprison someone in their home and to make them lose their sense of autonomy.

In terms of the data protection there are two points that I need to make. The first is that the Data Protection Act does not apply in relation to somebody's domestic activities. For better or worse, that includes abusive activities if they are doing that in their personal domestic capacity. The regulation does not reach them. That is not to say that these devices and



HOUSE OF COMMONS

those behaviours are unregulated, but those are matters for the police and I think that they are capable of being addressed through the criminal law. Abusers will choose any technology they can to manipulate and control the object of their abuse.

Q303 Simon Jupp: Is there a bit of a grey area here? Do you think that there could be work done to improve it, so there is a clearer line you simply cannot cross? I take your point and I know that police forces do use these situations in various cases, with domestic abuse cases, but do you think that there is more work to be done to ensure that legislation is up to date, given the widespread use of these devices?

John Edwards: I am not aware of a legislative gap. I do think that there will be cases in which police forces are ill-equipped to help a victim navigate the technical settings that they need to do to reclaim their autonomy and their control over those devices, for example. We know that beat cops may not be hugely technically savvy, and so while they can press charges against somebody who continues to harass and intimidate, they may not be well placed to assist a victim to engage with the provider, to reset the security settings and the like.

Stephen Almond: The point here around the Data Protection Act also extends to what is the right tool for the issue at hand. I query whether data protection would be the most effective remedy for what will frequently be criminal behaviour.

Q304 Simon Jupp: We know that this technology is incredibly clever, and it monitors how we do things, what we do and how we react to different scenarios. There is an issue of course that if someone is controlling that scenario, so controlling your heating or lighting or other stuff, and having access to the way that you live your life, if that situation changed the technology may not always change with it. It might get used to certain habits, for example, and I know that you can change settings, but is there a concern that it could leave people who have survived this abuse with a never-ending situation?

John Edwards: There are real challenges when you have a persistent and determined abuser who knows enough about the target of the abuse to essentially engage in identity theft and to continually inveigle their way into their victim's lives.

Q305 Simon Jupp: These things build up a data profile and it could be regarding insurance, banking, stuff like that. It could mean that this just goes on for way too long.

John Edwards: These are challenges to providers of a range of online services. For example, if you have been living with somebody for a period, you learn a lot about them. You often learn enough to navigate past the security settings that third parties such as energy providers and telecommunications providers set up to protect people. The behaviours that these people engage in will often involve removing autonomy, so



HOUSE OF COMMONS

making sure that those services are only in their name, excluding the victim from the ability to control the services or their environment.

Q306 Simon Jupp: Are individuals' data rights sufficiently well drafted in your view at the moment to take into account the needs of survivors, the people who have been going through this, or is there anything that could be tightened up and improved?

John Edwards: I do think that we see increasingly a sensitivity in service providers to the needs of people who experience domestic abuse. I do not see necessarily a gap in the legislation. The legislation provides high-level principles that serve well in an infinite number of informational transactions, and I have not seen a deficit in data protection law that exacerbates the problems that victims of domestic abuse experience.

Stephen Almond: I have nothing to add except to say that the information rights that people have do present a remedy in this situation, so considerations around rights to erasure, considerations around the accuracy of data—people being able to, for example, state subsequently that they have withdrawn consent for some of the processing that has occurred—will help remedy past wrongs in this space.

John Edwards: Once a provider's attention is drawn to the unique circumstances that a victim of this kind of manipulation has endured, it is incumbent on them to protect the data with higher security practices and standards. They might set a level of protection that is good for the vast majority of the population, but they need to be able to accommodate those who are particularly vulnerable in society. As a regulator we would be going to them and saying, "Given these circumstances, given that this person has told you of their vulnerability, you should have applied a higher level of protection and security."

Q307 Clive Efford: Thank you for coming to give evidence today. One of the three key areas of the Government's product security regime is about protecting, securing and validating data. Is this necessary because the device manufacturers have not taken their obligations seriously?

John Edwards: I am ill-equipped to answer that question. Stephen, are you able to assist?

Stephen Almond: As John has alluded to already, there is a real distinction to be made here between organisations that are manufacturing and importing devices, and people who are ultimately using those devices for the processing of personal data. Until recently there was an imbalance, but now there is a parallel set of requirements for both organisations, which should provide a double layer of protection.

It was always and remains the case that organisations that are processing personal data have obligations in relation to the security of people's personal data, and in terms of their acquisition of connected devices they should be thinking that through. That has always been the case and remains the case, but the additional line of defence around



HOUSE OF COMMONS

manufacturers that the Product Security and Telecommunications Infrastructure Act provides means that the obligations that manufacturers should have are now placed in law.

Q308 Clive Efford: The Government stated when they were introducing the Product Security and Telecommunications Infrastructure Bill, now Act, that the performance on product security was poor. We had evidence from Big Brother Watch. They explained to us what they felt, that there was a lot of noise made that was very positive around data security, but when it came to the application that protective measures were poor. A huge amount of money was being spent on PR, but people were not getting the protection they were being led to believe they were. Where do you see it, as the Information Commissioner, on that? Do you think the performance is poor, or do you think that the critics are wrong?

John Edwards: It is hard to know in the abstract what is being referred to there, but again I would say that a number of devices that are available on the market have poor security practices. If you sell a nanny cam or a video camera that is a connected device, so you can monitor it on your phone, that has a password set as a default to "password", then you have introduced a vulnerability into your home and into that situation. You can go online and look at a website called Insecam and look at some of these cameras in bedrooms, in workplaces, in domestic situations all over the world, because they have designed a scraping tool to identify URLs associated with that product and to exploit that vulnerability. I do think that the Product Security and Telecommunications Infrastructure Act will address some of those issues by requiring a higher standard.

Q309 Clive Efford: In terms of protecting people's data, I have just had a quick look on your website and admittedly it was not a deep dive, to see what information you provide for instance in practical terms for people to protect their devices. What I have found is it is more about people's rights to data than practical advice. Do you think that you are the right regulator to deal with product security?

John Edwards: What we will deal with is those who deploy the products in a commercial environment. For example, while we cannot necessarily reach the manufacturer of that camera that I have just described, if an off-licence or a counsellor or a psychologist or whoever buys one of those devices and installs it as part of their security framework, they are then subject to the Data Protection Act and the UK GDPR. Those laws set a general expectation and obligation on those people, who are described as data controllers, to ensure that data is protected by adequate security safeguards. If I find that they have not changed the default password from "password" and that their premises can be accessed by anybody with a connection to the internet, I will say they have failed to meet that most basic obligation. I am happy to send you some more targeted links to our website, but we do have quite detailed advice about what some of those security expectations are. Security is such a broad, encompassing



HOUSE OF COMMONS

topic that it is difficult to be absolutely comprehensive, but certainly practical examples include changing default passwords.

- Q310 **Clive Efford:** I was interested in your answer earlier about smart tech that you use yourselves. Do you have these devices such as Alexa that allegedly listen to you all the time? Do you leave them switched on? What is your habit in how you use those sorts of devices?

John Edwards: They do not work unless you leave them switched on.

- Q311 **Clive Efford:** You can switch them on to use them.

John Edwards: You can, but it defeats the purpose of having something you can use on voice command. I am not that concerned. I will ask mine to play the news or play some music for me, or I will just broadcast my radio through it. Sometimes I will ask it to set a timer when I am boiling an egg.

- Q312 **Clive Efford:** The point I am trying to get at is that the fear of people with these devices is that they are scraping data and finding out information. Do you fear that?

John Edwards: I do not.

- Q313 **Clive Efford:** Can you explain why you feel that people's fears are unfounded?

John Edwards: I am not sure that everybody's fear is unfounded, but I am saying I have confidence in the products that I have chosen that they are not listening to comments that I make without the command preceding them, and that they are not recording, processing and using information from my flat in ways that are inconsistent with the undertakings that are on the privacy policy or written on the box.

- Q314 **Clive Efford:** The last question is, that implies the success of offices such as your own, that the monitoring of what is going on means that the people who manufacture these devices behave appropriately and do not exploit people's data in the way that many people fear.

John Edwards: The confidence that the market expresses in these devices partly reflects the expectation and belief that an office such as mine exists and is there to ensure that those devices are not used in unexpected ways, or that the data has not been used in ways that would be inconsistent with the foreseeable consumer expectation of the data flows and the use of the device.

Stephen Almond: One of the more exciting developments that I see in the market right now is organisations that are almost trying to outbid each other in terms of how to enhance people's privacy on connected devices. For example, with headsets there are concerns that if you are using a virtual reality headset or an augmented reality headset you might be picking up the personal data of bystanders who did not intend to be in the frame. Organisations are looking at how to get rid of that data as



soon as it comes into shot; how to make sure that they are removing all unnecessary processing and focusing purely on what is necessary.

There are other organisations that are thinking about how to increase better voice-activated signals, for people to be able to tailor their privacy preferences in relation to connected devices. That gives me quite a lot of hope that we are seeing a market that is evolving towards more mature privacy preferences, where people will be able to have greater control in future, but we need to be able to see more people shift in that direction.

Q315 Steve Brine: It is nice to see you in person, John, after your confirmation hearing with us, which thankfully went well, as you are here. I want to explore regulation of artificial intelligence with you. The Government have limited their approach to regulating AI, which I think is probably quite sensible. Instead of a bespoke definition, they have put the two characteristics, which you will know are adaptiveness, so systems that can adapt and expressly do things without programmed human intent, and autonomy where decisions are made without human control. That is their definition, for want of a better word. Are they right to focus on those areas? Do you think they are too narrow? What is your view on that focus, that definition?

John Edwards: Our approach to AI is that we already have a comprehensive principle-based legislative framework. It is technology neutral; it is capable of addressing innovations. I do think it is important to remain alive to developments, particularly in AI and designed unpredictability, for example. They present a challenge to the right to human review, but we have seen I think in the Bill a retention of the GDPR standard that people who are subject to automated processing should retain a right to have human oversight and intervention in those decisions. That is very important.

Q316 Steve Brine: Why is that important?

John Edwards: I think there is a tendency for overconfidence in the nature of the algorithms that is not necessarily independently validated. To have somebody say, "Look, I feel like I objectively meet all the criteria for accessing a particular benefit, but the machine has told me I am ineligible. I want somebody to inquire into it" is an important right to demonstrate accountability for the deployment of those systems.

Q317 Steve Brine: So literally "the computer says no" is a problem?

John Edwards: I think so, yes.

Q318 Steve Brine: But maybe sometimes the computer is more reliable than the human interaction.

John Edwards: There will be times and it is really important that we subject to very close scrutiny the algorithms, the vendor claims, the input data, the false positives and false negatives and ensure that somebody is accountable for the decisions that are made.



Stephen Almond: I will append to that. Our focus in terms of human oversight and review is in relation to automated decisions that have legal or similarly significant effects. We are talking about the big decisions here, where many people would say they expect to be able to question whether the algorithm has it right and have a second opinion.

Q319 **Steve Brine:** Give me an example. Medical?

Stephen Almond: Medical, or a recruitment decision might be an example of something where somebody might want an independent view as to whether the algorithm got it right in that context.

Q320 **Steve Brine:** Exam results?

Stephen Almond: Potentially. I think it would depend on the context.

Q321 **Steve Brine:** Where is the regulator in all this, in AI? What role do you think the regulator should take?

John Edwards: I think we have a standard-setting role. We have done a lot of work with the Digital Regulation Cooperation Forum. I am not sure how informed about that forum the Committee is, but that is a collaboration between the ICO, Ofcom, the Financial Conduct Authority and the Competition and Markets Authority. We are identifying cross-cutting issues. AI has been one of those and we are looking at, for example, or have issued, guidance on AI auditing as a significant product. AI remains on the work programme for the DRCF. We collaborate with the Alan Turing Institute and with others to ensure that we are aware of developments; that we are providing expert data protection input into guidance and standards.

Of course, we have a role after the fact. If there are deployments of AI solutions that create unfair outcomes, we have a jurisdiction to look into those, and we will. We have looked into some commercial offerings, in the recruitment field, for example.

Q322 **Steve Brine:** Can you give us an example of that? Can you talk about that?

John Edwards: We were told of a service that was being offered to employers that was a screening product that would detect using biometrics and AI. It was called emotion analysis. Stephen charitably uses the term "immature" for the technology. You might equally describe some of these offerings as snake oil, but there is not a sufficient scientific backing and there has not been sufficient assessment of the impact of things such as neurodiversity or different ethnic backgrounds. That is a space where I think we can be very effective and we can call out products that are offered to the market with unjustified confidence.

Q323 **Steve Brine:** This is about creating the space for the human condition to plug into the process?

John Edwards: I think it is a nice way of putting it.



Q324 **Steve Brine:** Do you see yourself as a facilitator of that space?

John Edwards: I think so. That is an elegant way of putting it. We do demand that the humanity is central to the assessment of the proportionality and utility of these kinds of products.

Q325 **Steve Brine:** Otherwise we are all Borg, aren't we?

John Edwards: Yes, quite.

Q326 **Chair:** On that cheerful note, I appreciate we are coming to the end of the session, I am mildly surprised that you seem quite relaxed about all these developments. You think that the companies behave well by and large, you have the powers and the capabilities to deal with it and that we should all be relatively relaxed about that. Is that an unfair characterisation of where you sit?

John Edwards: I want to assure the Committee that if I were apprised of a product, a connected device or set of services that represented real harm, I would act. I would act immediately and would prioritise that. What I am telling the Committee is that, while some of these devices do present challenges, particularly in relation to security, transparency and the ability to access some data protection rights, they are within the bounds of innovation that we manage on a day-to-day basis. We can meet those challenges under the existing legislation.

Q327 **Chair:** The other part of my question is about resources. Clearly you are having to regulate the biggest, richest companies in the world. Do you think that you have the fire power to do that if, as you say, you came across something like that?

John Edwards: We work with the resources that we have.

Chair: That is a different question.

John Edwards: If you were able to procure more for us, we would do more. Let me say that I would not resile from a regulatory intervention based on an assessment of asymmetrical resources within a large tech company. I would set out what my expectations under regulation were. If they were not prepared to meet those expectations, then we would use the regulatory tools available to us under the law.

Chair: Thank you very much, gentlemen. Thank you both very much. That was a very interesting session and very informative.

Examination of Witnesses

Witnesses: David Kleidermacher and Leila Rouhi.

[This evidence was taken by video conference]

Q328 **Chair:** This is the second session this afternoon of the Digital, Culture, Media and Sport Select Committee. I am delighted to welcome, remotely, David Kleidermacher, the vice-president of engineering for Android and



HOUSE OF COMMONS

Made by-Google Security and Privacy, Google, which is a hell of a title to read out. Welcome, David. Also Leila Rouhi, the Amazon Alexa vice-president of trust and privacy, Amazon. Welcome to both of you. You are both waving and smiling, so that bit of technology works, which is a great relief.

Thank you both for joining us. You are both joining us from California and it is no doubt some ungodly early hour, so thank you particularly for getting up early to talk to us. I want to put it on record that we also asked Apple to join us and it declined to give evidence to this session. We are disappointed about that and want to say particular thanks to your two organisations for taking part. You may get some tough questions over the next few minutes or so, but we are very grateful that you are here to answer them.

Steve Brine: Hello, both of you, welcome to London and thanks for being here. Your two companies are the biggest and most renowned manufacturers of connected devices. Can you excite me—beyond smart speakers, which bore me immensely, I have to say. They do not interact with me, they do not talk with me, they do not make me laugh. I always thought that it was going to be like kit from Knight Rider, but it just tells me the time. Can you excite me about the future of connected tech? What can it achieve? What are you working on in the labs deep down beneath Google and Amazon?

David Kleidermacher: Thank you. I appreciate you having us here today to hopefully help in your inquiry. There is so much to talk about when it comes to the future of connected tech. It is front and centre with Google's mission to make information universally accessible and useful and helpful for people. I work in the security and privacy area and when you ask a question I tend to go towards areas around protecting people.

There are so many exciting things going around. If you think about healthcare, the ability to use connected tech to help us live not just longer lives but better lives, like ageing in place, so home healthcare is super exciting. I live in California and we have earthquakes. In Android we have built this advanced earthquake detection system in our mobile phones. Similar technology is being used to help augment in Ukraine, in the war, air-raid sirens through their phones. When you think about safety and your personal safety, that is an area that I find fascinating. There are so many things going on.

Q329 **Steve Brine:** Tell us a bit more about the personal healthcare side of things. There is a lot of talk here at the moment about winter pressures on our health systems. There is a lot of talk about virtual wards and people looking after their own healthcare remotely. That is an area that Google is very much working in. Tell us about what the future looks like in that space of connected tech, wearable tech.

David Kleidermacher: A lot of it comes down to how we enable this kind of connected technology to help people have fitness, have input,



HOUSE OF COMMONS

give people more information to help manage their healthcare, but do it in a way that is responsible. A lot of the research is in responsible AI and how we also process information locally. Wearables, whether it be wearables or whether it be your smart speakers or cameras that can maybe detect falls, how do we handle that data and process that data locally so that it is privacy sensitive? Give users the information they need, but in a way that respects their privacy. That is one of many exciting areas I am happy to go through more.

Steve Brine: That is great. Leila, from an Amazon perspective, show me the future.

Leila Rouhi: Thank you very much, I appreciate the opportunity to be here talking about these important topics today. I can say that at Amazon, particularly in the Alexa organisation when I work, our focus is on making customers' lives easier, more fun and more safe through the use of connected tech. The reason we invest in these products is because we do hear from our customers that they do have an incredible benefit from them.

One example we have seen recently throughout the pandemic is how people have been using connected tech to stay in touch when they could not be in physical proximity with one another. Similarly we hear from our customers the everyday conveniences of using Alexa, for example, to be able to control your homes, turn your lights on and off, control your thermostat and those little conveniences that add up and create a better and different customer experience in and around the home.

Most prominently, we have seen a tremendous amount of possibility when it comes to populations that are ageing or that have accessibility challenges. I know in my own household that that has been transformative. My 85-year-old father, through the use of connected tech, now does not have to go up and down stairs in the way that he used to. He can see what is going on around his home easily. Therefore, we see a huge amount of potential for customers in that arena.

Q330 **Steve Brine:** That is the easier and the safe bit of your three words. Tell me about the fun part. What is the fun part of the future that Amazon can show me?

Leila Rouhi: We see on our Alexa devices even today, for example, people using skills to play games, to listen to stories, listen to music, engage with programmes that are fun and interesting for them. We aim to help them to discover more areas that would be interesting for them.

Q331 **Steve Brine:** David, to come back to you, the building blocks of the connected devices—voice assistance, AI, the learning part of it—where does that fit on the maturity-of-technology scale? Is it in a really advanced place or is there a lot further that it can go? How will that develop over time?



David Kleidermacher: We are relatively early in this whole connected tech, IOT area. Various studies show that we are pretty early in terms of the number of connected devices and all the software that goes along with it. When it comes to some of the computer technology, it is quite advanced. Software is very capable and AI is incredibly capable, but we are still early in the journey. There are things like responsible AI that are massive investments in making sure that we do it right.

Q332 **Steve Brine:** Finally, give me an example. In the area of space travel, at the moment we can travel to the moon and very nearby planets. That is about all that we can do. We do not have the ability to travel at lightspeed, therefore we cannot travel at great distances within the human lifespan. However, if that changed, everything changes. In energy generation we have had some exciting news before Christmas around fusion generation of energy, but it is a long way from being usable yet. If we are at the start of the journey on the building blocks of this connected tech, what is it that you would like us to be able to do that you have not yet invented?

David Kleidermacher: You are asking this question more from a solving big problems perspective, but I tend not to be too much of a prognosticator on science fiction and where we are going because it is hard to predict. It is hard to predict how all this will evolve. I feel like the utility and the capabilities are going to be amazing. Connected cars is one example. There are so many. I mentioned healthcare. If I worry about the future, given where I sit in my career in Google, I worry a lot more about things like how do we do it responsibly.

Steve Brine: Leila, would you like to add anything to that? Then we will move on.

Leila Rouhi: I agree with David's assessment that it is still relatively early days. We have done a lot of invention in this space and had some achievements, but we have a long way to go. Our near-term vision within the devices orb is a home that works on behalf of the customer, and technology that works on behalf of the customer. That is where our present focus is.

Q333 **Simon Jupp:** Good afternoon or good morning to both of you. How confusing. After Steve's very, very energetic questioning about how fun these devices can be, I want to pour water on that a little bit by raising the concerns over privacy in particular. We know these devices collect significant quantities of data about users. Is this level of data collection and the subsequent privacy concerns inherent to the design of connected technology?

David Kleidermacher: Information is central to everything that we want to accomplish, but how we manage the information and process it is what is important. I give tremendous credit to the regulations like the UK GDPR and others around making sure that the fundamental aspects of data privacy—that the guardrails are set up and managed well. Things



like transparency and control are not just a good idea but they are the law and followed very well. Beyond that, those are pretty well worn these days and pretty well understood by many tech companies.

The future in data processing to enable these amazing experiences—it is important that we think creatively and we innovate in privacy-preserving technology. That is something that I am really excited about in this area. It was something that we announced at Google I/O, which is our major annual conference for the developer community. We announced something called protected computing. You can read more about it online, but protected computing asks how we deliver these amazing, delightful experiences in a way that allows us to process the data locally into other forms of privacy-preserving technology. For example, in the home I can process data from these continuously-on sensors that are enabling these experiences but process it what we call on the edge. Whether it be on your wearable or on your speaker, it is processed in the control of your devices and does not necessarily have to be shared or collected.

Simon Jupp: Leila, anything to add?

Leila Rouhi: I would agree. Thinking about privacy as a foundational part of product development and ensuring that we are doing our utmost to provide customers with transparency and control over their devices and device experience and making controls easy to use. Then, of course, using data responsibly and for the benefit of the customer to power and enable the experiences that we know that they love and that we want them to have.

Q334 **Simon Jupp:** As a politician I knock on doors, because around election time and throughout the parliamentary term you are trying to convince people to vote for you. One of the things that I have noticed in the last couple of years is smart doorbells and other things like that, which can record you. That is not a problem in my case, I couldn't care less, but some people do not want their data recorded, they do not want their profile recorded. How can you mitigate that in these products' design and is that a significant concern? Sometimes, depending on the shape and size of a house and how far away that is from a driveway, you can catch people wandering past. That is a bit of a concern, isn't it?

Leila Rouhi: We do build features into our products to take into account exactly the consideration that you raise. It is incredibly important that we give our customers the ability to protect not only their own privacy but also that of others. In Ring Video Doorbells, for example, we have privacy zones. A customer could, for example, black out certain areas of the camera's field of view that they should not be or do not want to be recording. In addition, we have motion zones that allow the customer to tailor what triggers a motion that then potentially triggers a recording, if the customer has a recording plan. Of course we put the customers in control on those recordings and give them the ability to delete them. They can later delete them at a cadence that they can select per device.



HOUSE OF COMMONS

David Kleidermacher: Similar features that are important for these kinds of products is the control of how they are collecting information or what they can see. The only thing I could add to that is over time what we want to do is be able to do more—back to the protected computing idea—to process the data locally. We have been working hard on our cameras to move that intelligent processing of information into the edge, or into the camera itself.

Q335 **Simon Jupp:** David, sticking with you, in 2019 your company had to apologise to an oversight because it failed to disclose the presence of a microphone built into a Nest device. Does this show that perhaps some campaigners are right to be concerned about this technology?

David Kleidermacher: That event was important because it showed the idea of transparency so that consumers have full awareness that both the sensors in the device and the data that is being collected is super important. I like to say that transparency is the tide that raises all boats and that event was important in raising awareness. One of the things that we have done since then—

Q336 **Simon Jupp:** Sorry to interrupt, David. Of course it raised awareness, but the point is how did this happen? You build a device, it is there and there is a microphone built into it. That has to pass through lord knows how many tests and rigorous procedures, and yet it was not clear it was there.

David Kleidermacher: It was just an error in the spec sheet. What we have done since then is we now publish—this is how you always continuously improve on these things—a sensors guide that documents all the sensors. That transparency is super important because now people can pressure test those claims much more easily.

Q337 **Simon Jupp:** I totally agree with you that transparency is important, which is why I am asking questions about it. You say that there was a problem in the spec guide, but what about the actual use of the system itself? When you are selling a product it needs to be clear what it has on it, in the advert, on the packaging and all that kind of stuff, never mind the spec guide, which is the more technical aspect of purchasing a piece of electronics?

David Kleidermacher: I could not agree more. When you look at GDPR, a lot of the guidance and regulations are around giving users information at the time of the access. We need to pool some of that upstream so that, as you say, at time of purchase there is more transparency.

As you are well aware, if we look at connected tech there is almost always an app involved to help manage that. What we are doing on Google Play with the app store is with all these IOT apps we now have a way for developers to be transparent and document, at time of download of the app, acquisition time, the data that is collected, how it is used and how it might be shared and all that. That kind of acquisition-time



transparency, I 100% agree that is what we need more of. We need more guidance and we need to push the market in that way.

With the data safety labels, as we call them, that is a huge step in the right direction. We are now working with the Connectivity Standards Alliance, which is the pre-eminent interoperability organisation in IOT devices, working with it on how do we bring that same level of purchase-time or acquisition-time transparency of data to devices, themselves, both apps and devices.

Q338 Simon Jupp: Understood. Leila, a couple of years ago there was widespread criticism of the idea of, for example, Alexa devices providing NHS information. Getting a GP appointment is quite difficult at the moment in this country, but I cannot say that I would particularly want to ask an Alexa device for health advice. That was quite roundly criticised. Do you think that it shows that some people just do not trust this technology? They trust it enough to have it in their homes but not for stuff like that, where you are asking very sensitive questions.

Leila Rouhi: Different people have a different level or use case for how they want to engage with connected devices. In that particular instant, it is important to clarify that Alexa did not receive any personal or private information from NHS. That capability was intended to allow customers to use their voice to access the same information that they would be able to access, for example, on the NHS's public website. Therefore, for many customers that was a useful feature.

I will also say that we have come a long way in terms of earning customer trust and helping customers to understand how our devices and various features work over the last few years. Trust is ultimately the foundation of everything that we do at Amazon, and we recognise that our customers have many choices when it comes to the devices that they use. It is up to us to earn that trust and continually be working to maintain it with our customers.

Q339 Chair: Leila, coming to you, I want to disagree with Steve, who asked the first set of questions. I do find my Alexa fun and exciting, but I also find it quite scary because I have no idea how much is being listened to or where all that information is going. What reassurance can you give me and the millions of other people in Britain, who are trusting enough to buy them but are still suspicious in the background of what is going on?

Leila Rouhi: First, I will say that I am very happy to hear that you are enjoying your Alexa device. We have built Alexa to in a lot of ways be proactive and obvious to the customer. There is a common misconception that Alexa is always listening. That is part of the reason that we have wake word technology and the blue indicator light.

The way Alexa works is that it looks for a keyword that matches the wake word that you selected for your device. That can be "Alexa" or "Echo" or a number of other wake words that we provide. Once that wake word is



HOUSE OF COMMONS

detected, then the intent of the customer, what you say, does begin to be sent to the Alexa cloud for processing so that we can respond to you, and is stored. We have the blue light indicator on the device to make it very obvious to the customer when that is happening.

You can also go into our privacy settings at any time and see exactly what Alexa heard and what has been recorded. We give our customers control over those recordings. They can delete them at will, they can choose for them not to be stored at all or they can set a predetermined cadence at which time they want those recordings to be deleted.

Q340 Chair: The other half of the worry is where is the information going, who is it being shared with and how can I have any control over that?

Leila Rouhi: The control is in the privacy settings in terms of you have the ability to delete that data if you do want to. In general Alexa is designed to continually be learning and evolving and getting smarter every day. We may use voice recordings to train speech recognition in our natural-language understanding system using machine learning. Our aim truly is to give our customers transparency over their Alexa device and also give them control so that they can ultimately control their experience and their data. We know that that is foundational to them continuing to use and engage with our products and services.

Q341 Chair: Presumably you recognise that it will only take one or two big episodes that suggest that information is flowing to places where people would not want it to, for there to be a mass revolt against having these devices in the corner of your room.

Leila Rouhi: We are incredibly mindful of that, and that is why we invest so heavily in ensuring that that does not happen. We know that if we have a trust-busting incident like that it would have major ramifications for our business.

Q342 Chair: Let me move on to what the UK Government are planning. They have said that they are going to reform data protection. Is that something that you, as device manufacturers, support?

David Kleidermacher: Certainly we support the objectives of data protection legislation. There seem to be ongoing discussions about the details there and we are staying close to it. If there is anything that we can do to be more helpful during those discussions, then we are here.

Chair: Leila, are you in favour of what looks like the direction of travel?

Leila Rouhi: Yes, we certainly support changes that uphold the UK's high standards for data protection.

Q343 Chair: Given that the whole connected tech universe is driven by data, would it matter to you, David, if the UK reform of data protection jeopardised data sharing between the UK and the EU?



HOUSE OF COMMONS

David Kleidermacher: I don't think that I am familiar enough with those aspects to give you a comment. I am happy to come back to you on that in terms of sovereignty of data and sharing.

Q344 **Chair:** That is the underlying principle, that presumably you would prefer a universal data protection regime. From your point of view, it would make your business life easier if you knew what was allowed and what was not allowed across different jurisdictions.

David Kleidermacher: Yes, certainly having harmonised standards is very helpful. This is feedback that we have provided to DCMS for years now around the code of practice for security and now with the app store code of practice discussion. A big part of our feedback, especially for small and medium-sized businesses, is that having harmonised standards is really important. If every country has a different set of rules, that makes it very difficult cost-wise to keep up.

Q345 **Chair:** Is it not just difficult cost-wise but also actively impossible? If you are marketing a device around the world, if there are radically different data protection policies in different jurisdictions, does that make it difficult? Leila, do you want to take that one first?

Leila Rouhi: Yes, certainly I think that consistency and unambiguous regulations are necessary, if not incredibly helpful for us. Ultimately, our aim is to ensure that we can continue providing a seamless and consistent customer experience and we know how to achieve that while also being compliant with the law. I will not comment on the specific details of what is being proposed here because we would need to examine the details, but I would be happy to have our team follow up.

Q346 **Dr Rupa Huq:** Our Government said that cybersecurity tends to be a bit of an afterthought for manufacturers. Would you agree with this assessment?

David Kleidermacher: I am happy to start. I would say that it is too often an afterthought, and I can explain why. It is not for malicious reasons. Companies will prioritise what they have a strong economic incentive to prioritise. At Google, given the scale of the services and products that we offer across the world and given that literally every single day, in fact as we sit here right now, we are under constant cyberattack, we have a very strong economic incentive, and have had that for many years now, to invest and be proactive about cybersecurity. For many businesses, until you have been attacked, which many of them have not been yet, they are going to be reactive because there are plenty of other things to worry about and prioritise in order to make their profits.

At the end of the day, that is why we need better transparency around the security and privacy quality of products, because that security and privacy ingredients label in front of consumers will cause them to make their purchasing decisions. Those purchasing decisions, if they are based



at least partially on security, will cause the manufacturers to have the right economic incentive to do better.

Q347 **Dr Rupa Huq:** Leila, it is one about consumer trust as well. Is product security an afterthought for you with these connected products?

Leila Rouhi: Certainly not at Amazon. We have hundreds of dedicated engineers and security experts designing secure products and ensuring the safety and security of our systems and servers. We know security is absolutely foundational for our customers and if we do not provide them with a secure experience, they simply will not use our devices and engage with them. We also have security teams that work across Amazon and can see and address larger security patterns and deploy solutions quickly. We have technical safeguards in place to detect and block suspicious log-ins, and our devices receive regular security updates to ensure that they are protected against the latest threats and vulnerabilities. Certainly in Amazon it is a primary consideration and a top priority.

Q348 **Dr Rupa Huq:** Where should the onus be? It feels as if there is a tussle between consumers taking responsibility to check the security of the devices that they purchase, and companies inbuilding those features before they distribute them. Where should the balance be?

Leila Rouhi: In my view, there is a shared responsibility across stakeholders. Certainly companies have an obligation to provide safe devices and to do that foundational work to ensure customer safety, but customer education also plays an important role here. The more customers know about how to protect themselves and how to protect their data, the more empowered they are, so there are a lot of benefits to customers also playing a role here.

Dr Rupa Huq: Should it be equal responsibility for both?

Leila Rouhi: I do think that it is shared. It starts with manufacturers. They have to make the devices safe, but customers should also be given choices and be educated on how to exercise those choices and what they can do to protect their security and privacy.

Dr Rupa Huq: David, whose responsibility is it?

David Kleidermacher: I agree with what Leila is saying about the shared responsibility, but we also have to give consumers the tools to make better decisions. Today if you are going to buy a television, you go into the retailer and you can compare things like the screen quality and audio quality. There are many things that are human-perceptible that you can make decisions about, but can the consumer decide or have any frame of reference for deciding on the security and privacy quality of those products? The answer today is no. Again, I commend the DCMS and Parliament, NCSC and others in this area of providing transparency, because I fervently hope that in a short period of time we will be going into the retailer and we will see not just labels on energy for your



television but also a digital label, an online label, that tells you the security quality. Then consumers will make better decisions. Manufacturers will start to compete on security features, not just speeds and feeds, if you will.

Q349 Dr Rupa Huq: Government-sponsored polling has showed that only 20% of consumers take any action at all to secure their connected device or even know how to do that. Only 20% of people check the length of time that it is supported from purchase. Regulators do have a role to play here, but what can industry and manufacturers like you do to help upskill these customers? A lot of people just buy it because it has the biggest number of inches or whatever or other flashy features and it is an afterthought for them as well.

David Kleidermacher: It is an important question. I believe the ingredients label is super important, but there is also a lot that we can do in the lived user experience of our technology, our devices and the apps that we use to manage them where we can do better at providing consumers with more useful information to understand their security and privacy posture and do something better.

For example, on Android we have built something that we call the safety centre, which is a central location for understanding your security and privacy stature, including the security update status. Instead of buried somewhere, like what is the date of your last update, you get more of a track-like protocol. We have green, yellow, red, and if it is yellow or red it specifically tells you, "Here are some things that you should do or think about". Yes, the ingredients label is important and more user experience aspects that make it easy to understand your posture and make simple decisions to get into a better place.

Leila Rouhi: I would agree with that. We certainly play a role here in terms of educating our customers and making privacy and security and the features that are available to them easier to access and easier to understand. That is an area that we are incredibly committed to. Similar to Google, we have an area in our app in Alexa, for example, where a customer can find and access all their privacy settings. We have similar areas in our other devices.

In addition to that, we include details on our product pages. For example, when a customer is purchasing these devices, we include education and touchpoints as the customer is setting up the device themselves, to give them some visibility into the different features and experiences that are available to them. I do not think that 20% is an acceptable number of customers, and it behoves us all to increase that number and ensure that our customers are educated in these areas.

Q350 Dr Rupa Huq: Exploiting lack of understanding is something that features in something else that we have come across in our inquiry, which is how we have heard that connected devices in the home can be used by domestic abusers in various ways—coercion, control, financially



monitoring people, spyware, all sorts of things. Is there any evidence that you can point to that product designers take these issues into account when they are designing products?

Leila Rouhi: I would be happy to start on this one. We take those topics incredibly seriously. We are aware that, as with any technology, there are occasional misuses or abuses of connected tech. That is absolutely not the outcome that we want for our customers. We have engaged in the United States with experts in domestic violence and tech abuse to understand the needs of these customers and understand what types of features and choices we can build to enable these customers. We believe that the technology that we create should empower users and not harm them. Again, it is something that we take seriously and do not tolerate.

David Kleidermacher: If I could add to that, a huge part of Google's mission is to make sure that technology works well for everyone. That means a lot of things. There are many ways that technology can maybe not be as good as it needs to be for different populations and demographics. This is one of those areas, where at-risk populations are ones that are maybe under-served throughout the tech community. Amazon and Google have made that a priority for quite some time.

There are many examples of it. One simple example would be things like the advanced protection programme, where people can opt into a higher level of safety and privacy in their Google accounts, and it has impacts on how your mobile device is used as well. We have things like comprehensive programmes to counter what we call stock adware and spyware that can be abused.

We are working on user experience of things. We go back to how do we have the user be better informed of risks. There are things that we can do in mobile devices to alert the user that there may be something going on. Maybe they have installed something on their device with physical access, like someone who might be at risk of domestic violence installs something on their device, how do they know that something is going on in the background? Notifications and visual indicators are an important part of helping people get to a better place.

Q351 **Dr Rupa Huq:** The evidence that we have had from academics implies that current products are not meeting the standards to protect survivors if you do extricate yourself from one of these bad relationships where there may be digital, physical or financial abuse, all these things. What would you say to that?

David Kleidermacher: In almost all these areas that we are talking about in terms of risks of connected technology, there tends to be this cycle where companies like Google and Amazon that are more resourced tend to innovate before the long tail of technology. What we need to do is take the lessons learnt and develop better standards. There are many good examples of that, like the security ingredients label, accessibility requirements and responsible AI, and this is another one. What does



good look like when it comes to protecting these higher-risk populations? Let's take lessons learnt and have public-private partnership to define better standards and have better transparency across the full tech world.

Leila Rouhi: I would add that I disagree a bit with that assessment. We have seen the opposite at Amazon. I can give you an example. We do work with domestic violence organisations, including work to support their missions when it comes to survivors. We have heard from them that connected cameras are one of the most requested types of devices for survivors, oftentimes when they are leaving a shelter and trying to re-establish their lives. Having the peace of mind of knowing who is in and around their home if they have a protection order, having that awareness if the person that they are seeking protection from is on the property, that is an incredibly powerful tool for survivors.

We can work with these organisations to donate devices and ensure that they are getting into the hands of survivors and that people fully understand how to use them. We also donate the subscription that goes along with the devices, because we know oftentimes survivors do not have access, for example, to credit cards or bank accounts.

We recognise that there are potential abuses and downsides and that it is imperative that we as technology companies work to minimise the potential downside and eradicate them, but we do believe that these devices ultimately can and should be a force for good.

Q352 **Dr Rupa Huq:** I remember I went to see a refuge in my seat at a secret location. I think I put their app on the phone that I had that year. They had a harmless-looking app that women—or it may not be a woman, I suppose, the person suffering the abuse—could put on devices and the person perpetrating the abuse would not know what it was. If it was clicked on with a thumb, it was a hotline to a national charity. That kind of thing could be built into basic non-smart devices even.

If statutory guidance was developed by the regulator to enforce these standards in the product security legislation, co-authored with domestic violence groups—you have hinted that there are discussions under way, but if it had that strong regulatory framework—could that be a way forward for your designers?

David Kleidermacher: In general having a regulatory framework for these things can be powerful. The challenge here—we have seen it with the PSTI Bill. It took four years from the point of practice being written, with lots of feedback from Google and others, to the point where we had the legislation recently. It can take quite some time to develop what does good look like and what is the standard of care that you want to legislate. We have to start with that discussion. That is the first starting point—what standard do you want to point to? It is not practical to say, "Hey, please do better here". We have to work together on that.



In area of the mobile stocking concept, the DCMS has started work with app store safety—which we spent quite some time providing feedback on. I am again pleased with the leadership role that the UK Government have taken in having these great discussions and issuing guidance. That is an example where we can have better guidance about the quality of apps and cut down on the malicious and stock adware in this area.

Dr Rupa Huq: Leila, statutory regulation?

Leila Rouhi: I would largely agree. Certainly regulation can and should be considered where there is a societal interest at stake. I know that we would be eager to engage and ensure that the regulation is drafted in a way that is incredibly thoughtful and regulates these cases and not the underlying technology. However, I will also say that we are not waiting for any such regulation. We already take these matters incredibly seriously and we are doing our utmost to prevent abuse from happening, even absent any regulation in this area.

Dr Rupa Huq: You are Amazon Alexa, not Amazon the sales side, because I have gripes with it, but that is for someone else.

Leila Rouhi: Correct, yes.

Q353 **Clive Efford:** Thank you for giving evidence today. I am going to come to the Product Security and Telecommunications Infrastructure Bill, but can I come back on answers you gave to my colleague Simon earlier on, Leila, about smart street doorbells that have cameras and record people? They can be definitely a force for good. I have had a number of incidents of street crimes that have taken place, one particularly serious, and they were used by the police to go and find out who was in the area, because they went back and knocked on the doors of people who had those doorbells. However, that does indicate that they do record the movements of people not just on the front path but on the street and in the wider area. It is all right people choosing to do this, but for people who get recorded, who have not bought those devices—I know this is at the lower end of the scale—is that just a choice that they do not have the opportunity to make, whether they are recorded on these devices or not? Is that an indication of where this tech is taking us? It is at the lower end of the scale, but in the future this technology is going to be infringing on the activities of other people who are not even aware that that technology is operating wherever they are.

Leila Rouhi: Also we do build features into the technology to ensure that awareness that that recording is happening, for example, does happen and to minimise any recording that is off property. We also instruct our users with guidance on how to install the device to ensure that they are doing it thoughtfully and are mindful of others' privacy. I spoke a little bit about some of the features that exist, including motion detection zones and the blackout feature. We also have indicator lights on the cameras, for example, so that somebody can see when recording is happening, as well as stickers that we provide to customers to put people on notice that



HOUSE OF COMMONS

there is audio and video recording. Our aim here is to empower customers with tools that help increase their safety, security and peace of mind. However, I acknowledge that customers also do have to use these devices responsibly and in accordance with the law.

Q354 Clive Efford: In theory, could someone use it for nefarious purposes to monitor what is going on in movements of people when they are going in and out of their house and who is moving in and around the street?

Leila Rouhi: It is theoretically possible, but that is not the primary-use case or something that we have seen much of. Customers typically do use these devices purely to monitor their own safety and security. In fact, it is quite annoying for a customer to get a lot of alerts that are not relevant to them, so customers tend to narrow down the recording to make it useful for them.

Q355 Clive Efford: That is interesting. On Alexa and Nest, they have to be voice activated. We have heard that they are not sitting there listening, at least according to the people who have given evidence today, but what other things do they pick up? If I walked into the room where there was an Alexa or a Nest, would it immediately identify that I had walked into the room with a mobile phone? Do the devices connect with one another and are they aware of each other?

David Kleidermacher: Over time there is obviously a lot of sensors and there is a lot of ability to detect things, not just the key words that interact with the assistants but also to detect things like falls and various other things. Some of those experiences will be important in enabling new-use cases like some of the home healthcare stuff.

The key question then is, as these sensors are interacting and information is being processed, whether it is done in a responsible way. I would point you to the Connectivity Standards Alliance, which I mentioned earlier. This is an area where I think that the Government should get more involved. It is a global standard on interoperability, where one of the big discussions is around security and privacy and how we make sure that information is not just interoperable between devices but kept safe and secure. The key is that we have these sensors and how do we make sure that the data and the processing is done responsibly.

Q356 Clive Efford: I think that was a yes, that it is aware that a mobile phone is present, but how much information is exchanged between the two devices?

David Kleidermacher: That is going to vary very much based on the application that is involved. The user experiences that allow you to have a phone call going on one device and then you may move into another room and have the phone call or the video call switch over to another device so that you can have this seamless experience. This is one of many, many experiences that are possible. Exactly how much data is moved or whatever is going to vary by the experience. I would say that that is not the most important question, meaning that if the data is being



HOUSE OF COMMONS

processed locally in the control of the user, that is great. If the data is shared to the cloud and is shared between service providers, that is where there needs to be a lot more guardrails around how that is done.

Q357 Clive Efford: I am sorry, I may not have asked my question precisely enough. It was simply if I walk into a room and I am not attempting to communicate with Amazon or Nest but I have my mobile phone in my pocket, are the two devices aware of one another and do they start communicating with one another? If so, what do they communicate? For instance, can it identify that it is my mobile phone?

David Kleidermacher: Certainly that is possible. You have situations where you might have just a Bluetooth connection between two devices and they can auto-detect each other and connect. That would be one simple example of two devices who would be aware and be connected.

Q358 Clive Efford: Sorry, but would I not have had to set that up for it to be Bluetooth or would it do it automatically? That is what I am getting at. How much information is the Alexa or the Nest soaking up from the devices that are just around it, without necessarily any password being used to set up a Bluetooth connection?

David Kleidermacher: If you turn off Bluetooth then it will not be able to communicate, but if you have Bluetooth on with these devices, then there is some amount of sensing that can happen regardless. For example, during the pandemic Apple and Google partnered on the exposure notification technology, which enabled people to detect dangerous contacts. That was done through Bluetooth proximity in a privacy-preserving way. No data was sent to the cloud, it was all done locally. That is enabled by having Bluetooth on and of course the user would opt into that, but once you have opted into that the capability of detecting dangerous contacts is there.

Q359 Clive Efford: Exactly, but the question is how much information can be absorbed without me being aware of it? I am just in the presence of this device; how much information can Alexa or Nest absorb from my mobile phone?

David Kleidermacher: I would say that there is a general principle, which is that if data is not going to be processed locally, there has to be transparency and control over that. If data is collected to the cloud, that is different. Whereas if you are in the home some of these experiences where the devices are naturally sensing each other may be automated.

Clive Efford: I am conscious of time. Do you have anything to add to that Leila? If your answer is the same, we will move on.

Leila Rouhi: I don't have anything to add.

Q360 Clive Efford: The product security legislation broadly covers three areas—default settings, software updates and data security. Is that a sensible focus or would you focus in other areas?



HOUSE OF COMMONS

David Kleidermacher: The three are slightly different, but I take your point that it focused on three of the requirements from the original code of practice. Those three that were selected to prioritise make a lot of sense. However, the feedback that Google has given, and I personally have spent a lot of time with folks in DCMS for years now, is that rather than focus on exactly which requirements, although the three are very sensible, it is a matter of whether we can bring transparency to a larger set. Therefore, data protection is not one of the three. You mentioned data protection, but it is not one of the three.

That is a good example of one where it would be nice if a consumer who is selecting between products had transparency. Whether the product has encryption or not, the consumer should have the ability to know that. Therefore, the main gap and the main opportunity for improvement here is in having these digital ingredients labels with more transparency to enable consumers to compare and make better decisions.

Q361 **Clive Efford:** Would you say that this is something that needs to be covered in product design to improve the security of people in their devices?

David Kleidermacher: Of course, absolutely.

Q362 **Clive Efford:** Do you think that we do enough?

David Kleidermacher: In product design?

Clive Efford: Yes, that the designers and the producers of the products do enough.

David Kleidermacher: It varies widely and that is the whole point of why we need this. It is great that the UK Government have taken a leadership role here, but there is still work to be done to provide the transparency down to the consumer. I will go back to my virtuous circle, the cycle, where if you have better transparency that enables consumers to understand the differences in security, that will affect purchasing decisions and then manufacturers will prioritise because there will be an economic incentive to do better in the design. That will then circle back into the design process. Companies like Google, Apple, Amazon, we are pretty far ahead of most of the connected world. We need that transparency to drive the economic incentive for everyone else.

Q363 **Clive Efford:** In terms of security and software updates, how long do you continue to provide updates on your devices?

David Kleidermacher: The most important thing—sorry if I sound repetitive here—is that the consumer knows, at time of purchase, what the support timeframe will be. For example, with our Pixel devices and our Nest devices we have been for a long time now transparent in public about the commitment to security updates, the length of time for security updates, well before the PSTI Bill, which now includes that, so that a



HOUSE OF COMMONS

consumer can make better decisions at the time of purchase. It has been pretty rare to be public with that transparency.

The exact amount of time will vary from device to device. We support a minimum five-year commitment on our phones, on our Nest products. Over time that transparency will push manufacturers to make those lengths of time even longer.

Q364 Clive Efford: In terms of downloading and installing updates on devices, is that automatic? Can people continue to use your products without having to do security updates?

David Kleidermacher: It depends on the product. For smart phones, because there is a user interface where the user has control and understands the ability to control updates historically, the user is involved to approve that. That is typical also for IT equipment and laptops and things. For some of these connected devices where there may not be a user interface and the user is not interacting with it in the same way, you want those updates to be automated and that is how they usually happen.

Clive Efford: Leila, on all of that, do you have anything to add from your perspective?

Leila Rouhi: Yes, I would add that Amazon too discloses to customers the minimum length of time that we will provide security updates to their devices. Oftentimes we continue providing updates. Our original tablet, for example, from 10 years ago still receives security updates. I agree with the point on transparency.

Back to your earlier question about whether these are sensible areas, we do believe that they are. It is certainly not in our interests for our customers to doubt the security or safety of our products. It is important that there is a level playing field in terms of security standards and we think that this Bill will help to ensure that consistency.

Chair: Thank you, Clive. Final set of questions from Kevin Brennan.

Q365 Kevin Brennan: Thank you, and welcome to both our witnesses. Can I ask you about competition with China, in particular in relation to connected devices? How would you categorise that issue to both of your companies?

Leila Rouhi: At the risk of sounding like corporate speak here, I will say that we are not particularly focused on China. We strive to stay focused on our customers and providing the best possible experience for them. We think that is ultimately what drives customer trust and how they decide what products they want to purchase and engage with. While price is a factor, we think that ultimately by providing the best customer experience overall that is how companies compete and that is how they win, so that is our focus.



David Kleidermacher: If you are asking about consumer products that we purchase, going back to many things that we have talked about during this session, I would agree that we want consumers to make the best possible decision to protect themselves and to be in a safe and secure state. That means having these objective measurements, these standards of quality. It does not matter where that product is manufactured. In fact, you have products that are manufactured all over the world that may have components from other countries, and it is difficult to know where all the different pieces come from. However, what they can all have is an ingredients label that objectively explains the security quality, and that is what is most important.

Q366 **Kevin Brennan:** I know that we do not have Apple with us today, but have any of the disruptions at Apple's iPhone city in China affected your supply chains at all as businesses?

David Kleidermacher: Google does not have its core services—Google Play and YouTube and so on—in China, so there has not been any sort of connection that I am aware of.

Leila Rouhi: Not that I am aware of, but I am happy to follow up on that point.

Q367 **Kevin Brennan:** As a Select Committee we visited Korea last year and heard that theft and infringement of IP was a very serious issue with manufacturing in China and competing with Chinese firms. Is it a problem that you have had to deal with at all?

Leila Rouhi: Not in particular. To my knowledge, for Amazon devices that has not been an issue that we have focused on.

David Kleidermacher: The only thing that I would speak to that relates to this is that we have had—I mentioned earlier that we are under constant attack and one of those areas is state-sponsored attack and threats, including from China. Those have been reasonably well documented in the public domain. We work very, very hard and I would say that we have built maybe the world's leading security program to defend ourselves and defend our infrastructure against state-sponsored threats. That is maybe the one thing that relates to it that we worry about.

Q368 **Kevin Brennan:** For us as policymakers, what should we do to try to make sure manufacturers are not undercut by insecure, unsafe or cheap, unreliable products? Would you have any policy-making recommendations for us?

David Kleidermacher: Yes. Maybe to amplify what I said earlier, first the PSTI is a great step in the right direction and the UK is very clearly taking a leadership role among nations across the globe. What is still left to be done is how do you communicate that quality, what does the actual digital ingredients label look like to the consumer and how do we do that in a way that is harmonised across the world so that you do not have



1,000 different labels across all the different jurisdictions, and have a monitoring regime.

I mentioned earlier the Connectivity Standards Alliance. I would invite agencies from the UK Government to get more involved in that, because that monitoring and knowing that devices that might claim they meet requirements continue to meet them and can be pressure-tested by researchers, is across the board probably the missing piece. We need the transparency across more requirements and to have that be something that the world can pressure test and have transparency in. We are going in the right direction, but there is still a need for improvement.

Kevin Brennan: Anything to add to that, Leila?

Leila Rouhi: No, thank you.

Q369 **Kevin Brennan:** Okay, that is fine. Finally from me, Leila and then David, are you looking forward to living in the metaverse?

Leila Rouhi: I will concede that I do not know a lot about the metaverse. Certainly within the Alexa organisation, our focus has largely been the here and now and how we can enable and benefit customers in their homes. Certainly the technology is interesting, and I am eager to see it develop and to get a better understanding of what is possible.

Kevin Brennan: David, how about you? Is that a prospect or future prospect that you are looking forward to?

David Kleidermacher: Not really. It is not something that I think about much, the metaverse. I am very excited about certain kinds of artificial reality technologies, but the metaverse itself is not something that I think about.

Chair: Thank you. As long as we are all still living in our own reality, the same reality, can I say thank you very much, David and Leila? You have been very generous with your time and we have covered a lot of very important material that will contribute greatly to our inquiry and the eventual report. Thank you very much for joining us this morning from your point of view, or this evening from our point of view. That concludes this session.