HOUSES OF PARLIAMENT

Joint Committee on Human Rights

Oral evidence (virtual proceeding): The Government's response to Covid-19: human rights implications, HC 265

Monday 4 May 2020

Members present: Ms Harriet Harman (Chair); Lord Brabazon of Tara; Ms Karen Buck; Joanna Cherry; Lord Dubs; Baroness Ludford; Baroness Massey of Darwen; Dean Russell; Lord Singh of Wimbledon; Lord Trimble.

Questions 15-26

Witnesses

II: Matthew Gould, NHSX, Department of Health and Social Care; Elizabeth Denham, UK Information Commissioner, Information Commissioner's Office; Simon McDougall, Executive Director, Technology and Innovation, Information Commissioner's Office; Dr Ian Levy, Technical Director at National Cyber Security Centre.

Examination of witnesses

Matthew Gould, Elizabeth Denham, Simon McDougall and Dr Ian Levy.

Q15 **Chair:** With the issues very well aired and set up by our last two witnesses, we now move to our second panel, who are basically the man and the woman in the hotseat: Elizabeth Denham, the Information Commissioner, whose responsibility is data protection, and Matthew Gould, the chief executive officer of NHSX, who has responsibility for devising the rolling out of this contact tracing app. We are particularly grateful to both of them, but especially Matthew, because he is doing the Downing Street briefing this afternoon. It is really to your credit, Matthew, that you have subjected yourself to scrutiny by us on a day when you are going to be in Downing Street doing the briefing. Do we have Matthew with us yet?

Matthew Gould: Yes, you do.

Chair: Thank you very much for joining us. My first question is to you. How will this contact tracing app work? Obviously it is really important

that we all understand what it is going to do, because we are all going to be asked to sign up to it. What data will be collected? How will it be stored, and what will it be used for?

Matthew Gould: Thank you for inviting me. I am very glad that we are airing precisely these issues, because if we are to get the level of engagement that we need with the public we know that we will need to win their trust, which means dealing with precisely the issues that you are probing with us.

I will start with how it will work. Essentially, once you download and install the app it will start logging the distance between your phone and other phones nearby that have the app installed. It measures the distance using a form of Bluetooth that is less energy hungry than normal; it is called Bluetooth Low Energy, appropriately. That will store a log of proximity information on your phone. It is worth saying, because this is pertinent to questions of privacy, that at this stage the app does not know who you are, who the people you have been near are or where you have been. We are not saying that people have to give personal information to use the app, but we are asking people to enter the first half of their postcode, which is not nearly enough for us to have any idea who they are but is enough for us to be able to usefully tell geographically where we might be building up hotspots and issues that will help in managing the crisis.

The app gives every app user a rotating, randomised identifier. It does not know, if I have the app, that I am M Gould; it knows me as a number. If I come close to you, it does not know it is you; it knows you as a number. All it has is these matching pairs of identifiers. They will then be stored on my phone, and on your phone if we both have the app. Then, if I become ill with symptoms of Covid-19, I have a choice about allowing the app to upload that information. That in turn will trigger a notification which the NHS can send, anonymously, to other app users with whom I have come into significant contact over the previous few days. That is at the heart of it.

I will say a couple of other things that I think are important. First of all, we have put privacy right at the heart of the app and the way it works. It is designed so that you do not have to give it your personal details to use it. That is really important: it does not know who you are, who you have been near or where you have been. Secondly, the app is voluntary. You need to choose to download it, to enable it, to upload your data if you become symptomatic. You can always choose to delete it.

Thirdly—this is the theme we will develop later at the press conference—the app is not by itself a silver bullet or stand-alone solution; it is part of a wider strategy of test and trace, and it makes sense as part of that, sitting alongside testing and more traditional contact tracing. That last point is really important, because it is the link to contact tracing that means that, whether you have the app or not, the wider strategy serves the whole population, because we are acutely conscious that not

everyone has a smartphone and not everyone can or will download the app. It is by embedding it in the wider strategy, alongside more manual contact tracing, that we can ensure that we do not leave people behind.

The very last thing is that we tried really hard to take an approach based on transparency. We have said that we will open-source the code, we will publish the privacy notice and the privacy assessment, and we will publish the privacy and security models. We have been publishing blogs to set out what we are doing. We are doing all of this at enormous speed, so we have not done it quite as early as we would like, but we set up an ethics committee, chaired by Jonathan Montgomery, the former head of the Nuffield Council on Bioethics. We work very closely with the Information Commissioner. We are trying very hard to do the right thing in the right way.

Q16 **Lord Brabazon of Tara:** Mr Gould, I am speaking to you from the sunny Isle of Wight, which is about to find such fame as it has not had for years and years. I am holding my smartphone in front of me. I am looking forward to hearing when I will be told what to do and when to download the app, which I will willingly do. Can you say, though, what percentage of the population need to download this thing to make it effective? Will there be a lower age limit with regard to people downloading it? What about the over-55s, only half of whom, I am told, have smartphones? They are perhaps the most vulnerable group. By the way, the Isle of Wight is above average age.

Matthew Gould: First, the Secretary of State will discuss some of the details of the timing for the Isle of Wight phase at the briefing at Downing Street shortly. However, it is worth saying now that we are profoundly grateful to the people of the Isle of Wight for their participation in it. It is precisely by seeing how it works—doing this for real and seeing how the different bits of the strategy slot together—that we will be able to make sure that we iron out issues and get the hinges right between the different elements. It is an important moment for making sure that the strategy works as we need it to.

On your question about the percentage required for it to work, we do not have a minimum percentage. We have seen that in other countries, including Australia, Singapore and Norway, somewhere above 20% of people are downloading it. Even at that level, the app starts to give us some really important insights into symptoms, how the virus is spreading and how we need to deal with it. Even at that level, we still get great value from it.

If we can get to higher levels of participation—40%, 50%, or above—the app can make a big difference in identifying people who have been in touch with cases of Covid-19, or suspected cases, and making sure that we can identify and isolate those people earlier, faster and more effectively. That starts to materially affect our ability to remove, with confidence, some of the restrictions that people have been living under.

This goes back to the point that this is designed to be not a stand-alone tool but part of a strategy. It is precisely by embedding it in a strategy alongside contact tracing that we can be confident that, whatever level of the population has the app, we are doing this in the right way and capturing the contacts we need to capture.

On the age of users, we hope that as high a proportion of people as possible will download it. However, I am conscious that smartphone use goes down among the more elderly of the population. Again, that is why we need to make sure that this is part of a strategy alongside contact tracing, so that we are not reliant on just the app. It needs to sit alongside and be supplemented by contact tracers who can speak to people who do not have the app but who none the less may have come into contact with cases of Covid-19, or developed symptoms.

In relation to young people specifically, we will take advice to make sure that we get this right. We are speaking to the Information Commissioner and will speak to the Children's Commissioner, because it is really important that we get that call as right as we can. The honest answer is that we do not yet know what the answer is; we are trying to work it out.

Chair: So it might apply to children as young as 10 or 11. Is that right? How old are children when they get smartphones now?

Matthew Gould: My daughter is nine and is lobbying for a smartphone already. For the Isle of Wight, we are asking people over 16 to download the app. We will take advice on what to do for those under 16. I do not want to say precisely what the right answer will be, because we need to speak further to the Information Commissioner and speak to the Children's Commissioner and really try to work that out.

Chair: If this is all so anonymised and safe, why would you worry about a 12 year-old downloading the app? It seems a bit of a contradiction to say that it has no problems but that you somehow have to protect children from it.

Matthew Gould: First, this is new technology. There are a lot of countries and companies trying to develop it and deploy it at scale, and some already have. However, we do not yet know exactly how it will work; we do not know all the consequences. There will be unintended consequences and there will certainly be some things that we have to evolve. We need to level with the public about the fact that when we launch it it will not be perfect and that, as our understanding of the virus develops, so will the app. We will add features and develop the way it works.

In that context, we need to think through what the consequences might be for children. For example, a user might get a message that it might be reasonable to expect an adult to process, but which could be really scary for a child. It is not that we have identified particular issues that might mean that children should not use it, but there is an additional obligation

on us to make sure that we have really thought through all the angles of what it would be like for a child to use the app—how the messages and understanding will land, what the consequences will be, how it feels from the child's point of view—before we make that final decision.

Chair: Thank you. We turn to Dean Russell for our next question.

Q17 **Dean Russell:** Thank you, Chair. I thank both witnesses for being here. To give a bit of context to my question, I have done a lot of work in the digital space over the last 20 years and have also lectured for the Institute of Data and Marketing, the IDM, and the Data & Marketing Association, the DMA, through that time. Obviously, GDPR has been a massive issue over the past couple of years.

That is the context to my question, which is about the data usage within this. What sort of data will be collected? I appreciate that this will be very anonymous at the moment, but is there a risk of creep over the next year or two? At what point will that data end its life? Does it get deleted once it has been used and somebody gets a ping to say, "You've been in close proximity to somebody's phone and you should therefore get checked out", or does it continue to be stored somewhere? How could that data be used again in the future? This is not just about how it is used now but about how you anticipate the data privacy and data protection working in the longer term. How will the data be stored and used?

Matthew Gould: We have set out the very minimal collection that we will do now. We have said very clearly that we will explain in plain English any changes that we make. If, for example, we move to giving people a choice to offer more data, which could be useful, we will make it a choice and explain it very clearly. Our best defence against creep, as you describe it, is transparency and an assurance that we will do what we do openly and that sharing further data will be on the basis of choice.

You asked specifically about what happens to data if, for example, somebody chooses to delete the app, or at the end of the crisis. First, if users delete the app, all data stored on their phone that has not already been voluntarily shared with the NHS gets deleted. It is automatically deleted from the phone on a continuous, 28-day cycle.

If data has been shared with the NHS by choice, it can be retained for research in the public interest or for use by the NHS for planning and delivering services. Obviously, that would be done in line with the law and on the basis of the necessary approvals required by law.

Dean Russell: Can I just ask Elizabeth Denham that question from an ICO perspective?

Elizabeth Denham: From an ICO perspective, we know that the law was designed to flex in a time of emergency, but we play a very important role as the independent regulator in looking at the app in its design phase and in monitoring each iteration of the app and making sure that it does what it says on the tin.

The other really important part of our role as the independent regulator is doing a robust audit of how the app has performed and whether offboarding or deletion of obsolete data is taking place. In a sense at the front end, in the design of the app, we are a critical friend and we can give peer-reviewed technical advice to NHSX, as we have done. Matthew came to me very early in NHSX's thinking about the app to make sure that there was assurance going forward, because all of us expect digital tools to be used.

We have seen digital tools being rolled out for tracking and tracing around the world. There is a lively debate about centralised versus decentralised, and we can get into that, but it is important that there is an independent oversight body to look at what is happening and to make sure that it is being rolled out in a way that is effective but that also protects the public interest in privacy and security.

Dean Russell: Given that you have been involved in the development of the app, do you consider the ICO to be the independent body able to do that?

Elizabeth Denham: We consider ourselves to be the independent body because we are not sitting at the design table. We have been given some technical material, and we have looked at it. We expect to look at the data protection impact assessment, which is the key document for us to critique and comment on. We also expect to monitor how the public respond to the app when it is rolled out. We will take complaints and do investigations and audits, but it is also really helpful that NHSX wants to talk to the independent regulator at the design phase to make sure that privacy and security are built in. However, we are not across every document and every plan about what is coming next. We can play both the expert adviser and the enforcer.

Dean Russell: Thank you.

Chair: Following on from what Dean said, it highlights to me that it is quite difficult to be both invested in the design and development of this system—obviously it is to NHSX's credit that it has shared lot of details with you and asked for your input—and then to be policing and enforcing the right to privacy thereafter. Would you not then be criticising yourself if NHSX accepted your advice, but it turns out that it is not working in the way it should?

I want to press you a bit more on Dean's point that you are quite deeply into it even though you are not sitting around the table. How can you be both sharing the design and independently enforcing afterwards? It sounds to me as though it needs to be a separate person who has not been involved in shaping the design.

Elizabeth Denham: The model I am responsible for administering has us playing a role as an expert adviser, not just on this app, but on any innovation that is rolled out that has significant privacy impacts. The data

protection impacts come to our office to be commented on; we do not approve them, but we comment on them. This is not different from us looking at a new biometrics system or us commenting on the use of a new immigration tracing and tracking system. We give expert advice; we do not sign-off or approve something. If we did, that would conflict with us being able to carry out our audit and enforcement measures. The law that Parliament gave me to administer has us playing all those roles.

I am not sure how going out and trying to build another commissioner's office and another oversight body very quickly would work, given that we have to move at pace here. As I said, my roles are defined in law as being an adviser, commenting on new initiatives, enforcing, investigation, audit, and sanctions at the end of the day. We have powers, such as stop processing orders. We can do on-the-spot inspections without a court order. We have the ability to compel information from a public body or a private sector organisation, so we have broad powers to be able to carry out the full spectrum of our role. I do not think this takes away from me doing that.

Chair: Thank you. Baroness Ludford has the next question.

Q18 **Baroness Ludford:** Thank you, Chair. Ms Denham, you wrote a personal blog about three weeks ago in which you said that the starting point for contact tracing should be decentralised systems that look to shift processing on to individual devices where possible. The document on the ICO website, called *COVID-19 Contact Tracing: Data Protection Expectations on App Development*, makes the same point.

However, NHSX does not appear to be following that advice in the app that it is developing. I do not think it came out terribly clearly from Matthew Veale's evidence, but we understand that it is a centralised system. We also understood from Matthew Veale that it would not be that difficult to switch to decentralised. Why has NHSX not followed your advice? Lastly, when are you going to get the data protection impact assessment?

Elizabeth Denham: We expect to get it very soon; I have been told that by NHSX. NHSX has also agreed that we can perform a voluntary audit on the app and the system when it is appropriate to do so, so if we have a lot of complaints from the public, for example, the door would be open for us to do an audit. Matthew Gould has made it clear that we will have the ability to do that.

On the question about my comments in my blog and in the expectation document, we wrote that document to guide not just NHSX but other providers and developers that may be developing similar apps. It is a generic document about best practices. Since I am the Information Commissioner, if I were to start with a blank sheet of paper, it would start with a decentralised system. The Committee can understand from a privacy and security perspective why that would be so, but that in no way means that a centralised system cannot have the same kind of privacy and security protections.

It is up to the Government and NHSX to determine what kind of design specifications the system needs. It has to be based on science and what epidemiologists say about their needs. It is up to the Government to identify what those functions and needs really are. If they lead to a centralised system, the question the DPIA has to answer is why it is centralised.

My next question would be about how the privacy and security concerns are addressed. That is what a DPIA is: it is about the mitigation of concerns. However, in no way does my blog or my expectation document say that a centralised system is a no and that decentralisation is a yes. It is a spectrum.

The ICO convened OECD members and privacy authorities from around the world. We had 250 people on a Zoom call. It was fascinating to see the differences in approaches around the world. Many are centralised, in different ways, and many are decentralised. There is no one best approach. From a privacy and security perspective, it has to answer the question why and to identify the risks and how they are being mitigated.

Baroness Ludford: You said there is no one best approach, but your knowledge of the situation and the development of the app led you personally, and the ICO, to recommend a decentralised system. That goes back a little bit to the previous thread about whether you are more friend or critic.

You are the regulator; it is slightly worrying that, while you say you prefer a decentralised system, you sound a bit neutral between decentralised and centralised. That is slightly confusing.

Elizabeth Denham: Let me try it this way. We wrote an opinion after looking at the Google/Apple collaboration on the APIs. You will see that we put out a formal opinion on that; that is a decentralised system.

We said in that opinion that centralised systems can work, but they need to be able to demonstrate how the privacy and security concerns are addressed. I wrote that blog, that opinion and my expectations document before we had seen the detailed technical documentation and before we had seen the DPIA from NHSX.

As I say, if I start from a blank sheet of paper, I am a privacy and security expert. That is where I will start. The functionality of the app is up to the Government to decide, based on the evidence they have and the need in our communities. It is not for me to decide; it is for me to advise on how to mitigate some of these potential risks.

Matthew Gould: Would you like me to come in here to explain the choice that we have made?

Chair: Yes, please do.

Matthew Gould: First, if privacy were the only thing that we were optimising for, a decentralised approach could well be the default choice. But, actually, we are balancing a number of things. We are balancing privacy with the need for the public health authorities to get insight into what symptoms subsequently lead to people testing positive, for example, which kinds of contact are riskier, and what changes occur in the nature of contact between, say, three days and one day before symptoms develop.

Even on the basis of the system that I explained, where you are not giving out personal data it was our view that a centralised approach gave us the potential to collect some very important data giving serious insight into the virus, which will help us. In that context, we thought that an appropriate balance would be achieved in a system that provided both that potential for insight and, we believe, serious protections on the privacy front in the manner that I have described. As the Information Commissioner has said, it is really for us to work out where that balance is—to demonstrate that we have mitigations in place and have thought about the privacy side as well, as I genuinely believe we have.

I would make two further points. We are talking a lot to international partners. It is striking that, as the Information Commissioner said, there is a range of approaches, many taking a similar approach to ours.

Finally, a lot of this has come up in the context of the proposal put forward by Apple and Google and the technology that they have put on the table. We are working phenomenally closely with both companies. We are all dealing with a new technology and a new situation and trying very hard to work out the right approach.

We are not in competition. We are all trying to get this right. We are constantly reassessing which approach is the right one. If it becomes clear that the balance of advantage lies in a different approach, we will take that approach. We are not irredeemably wedded to one approach. If we need to shift, we will.

Chair: For me, the video froze at the point where you said, "If it becomes clear that a different approach …" Could you complete that sentence?

Matthew Gould: I apologise. If it becomes clear that a different approach is a better one and achieves the things that we need to achieve more effectively, we will change. We are not particularly wedded to a single approach. It is a very pragmatic decision about which approach is likely to get the results that we need.

Chair: What is the timeframe within which you can decide to go with one approach rather than another for locally held information? Once you have opted for one, presumably that is it.

Matthew Gould: I am not sure that is right. We will not lock ourselves in. If we want to take a different approach, we might have to do some

heavy-duty engineering work to make that happen. But I want to provide some reassurance that just because we have started down one route does not mean that we are locked into it.

Chair: Thank you. I now go to Joanna Cherry for the next question.

Q19 **Joanna Cherry:** Thank you, Chair. Mr Gould, whose decision was it to follow a centralised rather than a decentralised approach?

Matthew Gould: The team made recommendations and those recommendations were taken by the oversight board, which I chair and then report to the Secretary of State. To emphasise the previous point, it is not necessarily a decision for all time. We will keep it under constant review and do our best to make sure that if we need to change, we will.

Joanna Cherry: We are a bit pressed for time today. Would it be possible for you to write to the Committee and tell us who is on the team that took that decision?

Matthew Gould: Of course. Ultimately, the oversight board is responsible for making recommendations like that.

Joanna Cherry: I noticed that in your evidence to the Science and Technology Committee last week you were asked whether GCHQ had been involved in the decision-making. You said that it had. Was it specifically GCHQ that wanted a centralised data-collection process?

Matthew Gould: No, and it is worth saying that the involvement has been through the National Cyber Security Centre, the national technical authority. We have been very glad to have its expertise, to make sure the system is as privacy-enhancing and security-protecting as it can be.

The advantages of a centralised approach are really about the public health advantages that I talked about earlier. It is the ability, without knowing who the individuals are, to see some of the patterns that will tell us important things about the virus.

If you have a centralised approach, it becomes more straightforward to hone your understanding and decision-making inside the app, which will allow you, for example, to make sure that symptoms become more accurate over time and you get a better understanding of when the most dangerous time in somebody's development of symptoms is for them to be having proximity events. Over time, it will tell us whether, for example, five minutes at one metre away is rather more important than 15 minutes at two metres away. These are all epidemiological advantages that we believe our approach will allow us to exploit.

Joanna Cherry: I see that a number of other countries in Europe, including Germany, Switzerland and the Republic of Ireland, have gone for a decentralised app. In our previous evidence session we were told by Dr Veale that a centralised app one side of a border will not be interoperable with a decentralised app on the other side of the border. Is

it not true that the UK's decision to use a centralised app will cause problems for interoperability across Europe and particularly on the island of Ireland, where two different apps will be operating on either side of the notional land border?

Matthew Gould: Just to be clear, even in Europe it is not just us who are taking this approach; the French, for example, are taking a similar approach. We are worried about interoperability, so we have convened international partners to look at interoperability and to work out how we can make sure that it works best across borders. These things are never straightforward; to try to get these complex new systems on the new technology or to talk to one another will be no small task. The point is a good one, and we are trying to work through how it can best work.

Joanna Cherry: It will be a particular problem on the island of Ireland, will it not?

Matthew Gould: It raises a further question about interoperability that we will have to work through.

Q20 **Joanna Cherry:** May I ask you a couple of questions about the data storage, which individual members of the public will be interested in? Once somebody decides to upload their diagnosis, what happens to their data once they notify the app that they have been diagnosed with Covid-19?

Matthew Gould: The data that they upload, which is a set of matching pairs of randomised IDs—to be clear, we are not talking about personal data but about pseudonymous data—will be stored securely, and it will allow us to hone the alerts that are at the heart of the system.

Joanna Cherry: Will it be possible for a person to be identified by name as a result of the data sent to the central system?

Matthew Gould: It should not be, because no personal details are attached and the data is held securely. People can use this with confidence that they will not be identified personally.

Joanna Cherry: Why do you need the first half of the postcode, as mentioned earlier?

Matthew Gould: We chose that very carefully. On the one hand, it allows us to know, for example, when there is a growing issue of proximity events and a potential spread of Covid in particular areas. It is broad-brush enough to know, for example, that a particular hospital there will need to prepare itself for a potential upsurge in local cases. But it is also broad-brush enough to make sure that there is no danger of it identifying individual people.

Joanna Cherry: Once someone's data has been sent to the centralised collection area, can that person request that their data is deleted?

Matthew Gould: No. The data can be deleted as long it is on your own device. Once it is uploaded, it becomes enmeshed in wider data, and the technical difficulties of deleting it at that point become tricky. It is also worth saying that, at the end of the crisis, all the data will either be deleted or fully anonymised in line with the law, so that it can be used for research purposes.

Joanna Cherry: Will that assurance that that data will be deleted after a certain amount of time be written into law? Have you discussed that with the board or the Government?

Matthew Gould: It is a commitment that we are making.

Joanna Cherry: What legal guarantees will people have that that commitment will be honoured?

Matthew Gould: One legal guarantee is the basis under which we have been doing this in the first place, which is obviously in the context of a health emergency in which particular rules apply. I defer to Elizabeth on the precise details of it under law. However, once the health emergency has finished, the basis for us having the data changes, so there should be a sufficient guarantee there.

Joanna Cherry: Okay.

Elizabeth Denham: Data protection law is flexible enough and has strong enough principles and provisions to cover all these aspects. The issues of obsolete data, the deletion of data, and turning any identifiable data into anonymous and deidentified data before it is used for research are all covered by the Data Protection Act 2018.

Joanna Cherry: But it is correct to say, is it not, Ms Denham, that other rights than just privacy may require protection here?

Elizabeth Denham: That is correct. Some pieces of law in this area intersect, such as employment law, human rights law and privacy law. However, if we are talking specifically about the data and whether or not it needs to be deidentified to be used for research, all issues that are specifically about data are dealt with in the UK's data protection framework of law, including the GDPR and the Data Protection Act 2018.

Joanna Cherry: Mr Gould, I have a quick couple of questions about data storage. What about the data relating to a person who receives a notification that they have been in contact with somebody who has been diagnosed with Covid-19? How is any data related to that person stored?

Matthew Gould: In the same way. It is a fair question, and perhaps I might write to the Committee to give more detail about it.

Joanna Cherry: Finally, will it be possible for anyone to use the data generated to trace the movements of an identified individual?

Matthew Gould: No, because we are not collecting location data. The app does not know who you are, who the people you are seeing are, or where you are, so trying to use it to know where an individual is will not work.

Joanna Cherry: But it knows the first part of your postcode.

Q21 **Chair:** May I butt in with a question arising out of that? My mobile phone company knows who I am—my device is identified with me—so how can it suddenly be not known?

Matthew Gould: Because we are not taking the identifier of your phone. We are taking the make and model, which we need to know because different phones operate in different ways, so it is absolutely germane to the way Bluetooth operates. However, we are not taking your personal identifier from your phone, so your phone company will know who you are, but the app sitting on the phone does not.

Chair: At that point, I will go back to Joanna.

Joanna Cherry: I have covered all the points I want to cover at this stage, so we can go on to the next question.

Chair: Thank you. We turn to Lord Dubs.

Q22 **Lord Dubs:** Who will have access to the data? You mentioned the NHS, but of course the NHS is a large organisation. Which parts of the NHS will have access to data, and what about the Government as a whole? Will Apple and Google have any access, assuming that we have a centralised system, and what about the police, who for certain crimes have access to the phone of a complainant?

Matthew Gould: We have said clearly that the data will be used only for health, public health and associated research purposes. It will not be used for law enforcement. I cannot give you a definitive list of exactly who would have access to the data, but we will have proper procedures in place consistent with law that will make sure that only those who have an appropriate health or public health reason for seeing the data do so, and under very clear conditions and criteria.

Lord Dubs: So Apple and Google would not come into that.

Matthew Gould: No. I cannot see a scenario in which Apple and Google would have access to that data.

Q23 **Lord Dubs:** I think that you have partly answered my next question. Assuming we have a centralised system, will Apple and Google play any part in this process?

Matthew Gould: They will, because they run the two main app stores through which people will download the app. They provide a large number of the smartphones and other devices that people use. Whether we go for the model that we have chosen for now, which is the

centralised approach, or whether we change course, we will continue to work closely with them on the technology. That is not to say that we will share data with them, but it is absolutely right that we should talk to them about how we make sure the process works best. Given that we are sitting to a considerable degree on platforms that they have created, we should think together about how we solve this new and quite complex technological as well as medical problem.

Chair: Mr Gould, you said that only people with an appropriate public health reason will have access to the data. What if an employer wanted such access, the public health reason being to protect their other employees?

Matthew Gould: That is a very fair question; it touches on issues of law that I think I will need to consult on and perhaps write to you about. I can tell you what I think the answer is, but I think it best that I get an expert opinion and come back to you.

Chair: We know that the police ask complainants in rape cases for their mobile phones to check texts that might have gone between them and the alleged rapist, and they go through all the material on the mobile phone. What would happen in such a situation? Would they not see the notifications that had come from this system?

Matthew Gould: The notifications do not say whom you saw. They do not give any identity. If you get a notification that you have had a proximity event with somebody, it sets out only that you have had such an event; it does not say with whom, on what day or in what place. The information is still privacy enhancing.

Q24 **Chair:** Okay. Thank you. We go to Lord Trimble. Lord Trimble, are you there to ask your question? I will ask it as he seems to be offline at the moment.

When a person receives a notification that they have been in contact with somebody who has been diagnosed with Covid and it is suggested they self-isolate, will that be voluntary self-isolation, or will any enforcement be involved? Will any authority be notified in respect of the person receiving such a notification, or does it just go to them and depend on their good will?

Matthew Gould: As I have said, the system works on the basis that we do not know who the user is—the app does not know who the user is. If it sends out an alert saying, for example, "Somebody you have been in touch with has subsequently tested positive for Covid-19 and you should isolate", that goes to a randomised ID. We do not know who it is. Precisely for that reason, the system relies on voluntary compliance with that advice.

Over the last couple of months, we have seen a huge sacrifice by the public to make sure that we can save lives, protect the NHS and do the right thing. It is our hope and belief that such determination to help

protect the country, save lives and stop the spread of the virus will continue to power people downloading the app and, as appropriate, following the advice it gives.

Chair: I see that it is now five to four and we must let you go to Downing St, Mr Gould. I thank you very much for being prepared to answer our questions. Thank you in advance for agreeing to write to us on the questions you wanted to reflect further on before you gave an answer. Thank you, too, for your important work in trying to get us to a situation where the lockdown can be eased safely.

We have one final question to the Information Commissioner from Joanna Cherry.

Q25 **Joanna Cherry:** Commissioner, do you have an expectation of the role you will play when the contact tracing app is rolled out? We have touched on this already. I am interested in the provision of oversight and review of how the app is working in relation to its compliance with individual rights.

You have made the point already that from time to time you are asked to comment on matters relating, for example, to biometrics. Of course, there is also a separate Biometrics Commissioner. We heard evidence from legal experts earlier in this session today that it would be of benefit in relation to transparency and in dealing with the public to join in with this experiment, if you like; to have oversight by an independent commissioner; and possibly to set up a tribunal to which people could make complaints if there were to be any abuses of the system. Do you agree with me and them that such independent oversight would be desirable?

Elizabeth Denham: I know that there is already independent oversight of these issues. The Biometrics Commissioner, to take one example, has no powers of investigation and can only make recommendations. The same goes for the Surveillance Camera Commissioner. The only regulator in this space to do with data protection is the ICO. Our powers of investigation and audit are subject to oversight by a tribunal. We have the body set up to be able to take a complaint from the public, investigate and come to a conclusion. If there is disagreement or unhappiness with that conclusion, there is a tribunal that takes those complaints.

The advisory services that we provide do not mean that we cannot take complaints because, again, our advisory services are not signing off on an app. As I have said, we have seen some technical documents, but we have not yet seen the data protection impact assessment, which is critical for us to be able to see what legal bases will be relied on for the application. Michael Veale talked about this earlier. We have also issued opinions and best practices.

As for audit, as the app was rolled out and after it was decommissioned, we would look closely at exactly what data was collected and why, how

much transparency there was about the programme and what additional applications or features were added.

Right now, we know that it is a proximity and notification system. It is not a system that is connected to immunity passports and it is not one that people are compelled to download. We all want the app to work not as a silver bullet but as a plank in our ability to get back to work. I have told the Government that they need to be transparent to the public by publishing the DPIA and the code, and by giving us as the expert regulator the documents so that we can be a critical friend. They also need to stick to the disclosed uses. The devil is in the detail in the disclosed uses which the public need to understand. But we want it to work, and I am confident that I have seen a serious focus on privacy and security

Joanna Cherry: It is not just the rights to privacy and security that may be engaged by this data collection, because there are other rights and protections under the Human Rights Act and the ECHR which may be engaged. One example is the right not to be discriminated against. Your office has closely focused on protecting the right to privacy and to security, but given that other rights will be engaged, do you not see that there is an argument to have oversight that focuses not only on privacy but on other issues of human rights? Do you see my argument?

Elizabeth Denham: I can see that there are other areas of law and other types of oversight that would be necessary in order to think about discrimination in employment or discrimination of a vulnerable group. However, data protection looks at fairness, proportionality and transparency. Those principles are critical. The analysis of proportionality that goes into data protection is similar to the proportionality assessment and test under Article 8. There are some similarities between those two, and I can write to the Committee in more detail about that.

Joanna Cherry: Okay, but do you understand the argument that many members of the public are rightly concerned about the impact that downloading this app on to their phones and giving up their information to a state body might have not just on their privacy but on their right not to be discriminated against if they are, for example, LGBT or they are migrants? Do you see the argument that it might increase public confidence and therefore the uptake and utility of this app if there was an oversight body that is separate from yours that was focused not primarily on privacy and security but on the protection of all rights under the European Convention on Human Rights?

Elizabeth Denham: Yes, I can see a lot of ways in which we could increase the confidence of people who are concerned about these things. That is why it is so important that the Government are transparent about what data is being used, how it is used and why it is used. They have to make sure that the app is truly voluntary, and they must stick to the disclosed uses of it.

They must also minimise what data is collected so that it gathers only the information that is absolutely needed. That is why we got into the difference of using only the first three digits of the postcode as opposed to the entire postcode, because you will understand that that would be identifiable information. It needs to be truly voluntary, because otherwise I agree that the public will be spooked when deciding to download the app. However, we all want the app to work.

Joanna Cherry: I agree, and I would like to see the app work as part of a larger strategy. However, it is my duty as a parliamentarian to try to put people's fears about it to rest by addressing their right to protections. If we had independent oversight that was underwritten by a piece of legislation governing the app, the Government would have to make a statement under the Human Rights Act that that legislation was compliant with it.

Surely that would send a big signal to people that all their rights, not just their right to privacy but to their right for example not to be discriminated against, had been taken into account in the roll-out of this app. They would have not just the Government's assurance but a piece of legislation along with an independent and impartial commissioner like you but one covering a broader field to whom they could go if they had a legitimate grievance.

Elizabeth Denham: That is one for parliamentarians and government to look at. My focus right now is making sure that I do a fulsome job when it comes to data protection and security of the data.

Chair: Thank you. I will go to Dean Russell for the final question to the Information Commissioner.

Q26 **Dean Russell:** I have a couple of points of clarification. First, just so that I am 100% clear, as I understand it, on the data that the app will in effect be generating and collecting, apart from the first part of the postcode that is put in it will be completely anonymised in the sense that you will get no details about the individual apart from the fact that their phone has come into close proximity with another phone. Is that correct?

Elizabeth Denham: That is my understanding, but, again, we are waiting for the data protection impact assessment for a full analysis and we will also need to look how at the app works in the wild so that we can see how the collection is happening and whether that is synonymous data or anonymous data, which are meaningful terms. There is a lot of detail in our expectations document, which sets out best practices in the way that the app should work

Dean Russell: Thank you. That is my understanding from what I have heard today, so I hope that that is the case. My second question is related to that, but I think you may have just answered it. I understand that there are no plans for this app to work with other apps, so the data will not be interoperable or shared with other apps on an individual's phone, rather that it will be completely siloed and work alone. Is that the

case?

Elizabeth Denham: That is also my understanding from the technologist that we have been speaking to at NHSX. Again, however, having that key document, the data protection impact assessment, along with the requirement for NHSX to provide it to me and to the public, is a really important protection, especially when everything is happening at pace and we want the public to take up such an app in order to help with proximity and notification.

Dean Russell: Finally, do you have a sense of when that privacy notice will be shared?

Elizabeth Denham: The privacy notice and the DPIA will both need to be shared with us. I know that NHSX also plans to publish that, so that it can show the public that it is transparent and accountable for what it is doing. I think that is on the verge of happening, and we will all be interested in the results of the trial in the Isle of Wight and to see whether it is working in the way the developers intended.

Chair: Thank you very much indeed for giving evidence to us today. We thank you for your important role in data protection. You could quite fairly have said that Parliament has given you the responsibility to take on the advisory role and the enforcement role and to handle complaints, and you are discharging the responsibility that Parliament has given you.

The question now is whether, in the face of the big challenge posed by the importance of public perception, we think that the framework that I and other MPs were part of establishing some years ago is the right match for the current circumstances. I thank you again for your work and for giving evidence to the Committee.