HOUSE OF LORDS

Select Committee on Science and Technology

Corrected oral evidence: The science of Covid-19

Monday 6 July 2020

4 pm

Watch the meeting

Members present: Lord Patel (The Chair); Baroness Blackwood of North Oxford; Lord Borwick; Lord Browne of Ladyton; Baroness Hilton of Eggardon; Lord Hollick; Lord Kakkar; Lord Mair; Baroness Manningham-Buller; Viscount Ridley; Baroness Rock; Baroness Sheehan; Baroness Walmsley; Lord Winston; Baroness Young of Old Scone.

Evidence Session No. 14	Heard in Public	Questions 132 – 139

Witnesses

Iain Bell, Deputy National Statistician for Population and Public Policy, Office of National Statistics (ONS); **Dr Michael Veale**, Lecturer in Digital Rights and Regulation, UCL; and Digital Charter Fellow, Alan Turing Institute; **Hugh Whittall**, Director, Nuffield Council on Bioethics.

USE OF THE TRANSCRIPT

> This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witnesses

Iain Bell, Dr Michael and Hugh Whittall.

Q132 **The Chair:** We move on to the second session. I welcome the panel and hope that you are all there. Mr Bell, Dr Veale and Mr Whittall, thank you very much indeed for coming this afternoon to help us with this session. No doubt you have been listening to the first session, so you might have some comments to add when we ask our questions. We will start with Viscount Ridley.

Q133 **Viscount Ridley:** My questions are simply: what types of data are being collected to help manage the pandemic, and what organisations are involved in handling this data? I would then like to follow that up by asking about the privacy and ethical concerns.

Dr Michael Veale: I was involved in building the app that inspired Apple and Google to create their decentralised contact tracing system. We started building this in early March with eight universities. The data used in that system is Bluetooth contact data between devices. However, it is not clear that collecting data is always the best way to think of this system.

When you engineer certain types of systems in a privacy-friendly way, that data does not need to even leave your phone. It can be effectively used to deliver the contact tracing service using Bluetooth, but no other organisation has access to it—it remains on the device. If it was not done in that way, the data would be considered to be social network data—a map of who saw whom in society, including people who were not infected or at risk. That was the kind of data initially proposed by the NHSX app but not by many other countries. However, some countries, such as Singapore, will be using that. That is one type of data being used in the pandemic.

Other types of digital data are cellular data from phone masts. The UK has not indicated a preference to use that, but it could do so under the Investigatory Powers Act. It would have to argue the case for doing so, but it is arguable that it could do it. Another type is ultrasound data from the microphones of phones, and wi-fi data is commonly used as well.

Iain Bell: At the Office for National Statistics we have set up a number of surveys to help monitor the pandemic. As was mentioned in the previous session, we have set up the Covid-19 Infection Survey, which monitors the prevalence and incidence of Covid-19 within the community. On Friday, we published for the first time the results of a study into the prevalence of Covid-19 in care homes, and we sent links with that evidence to your Committee on Friday. That utilises data by going out and swabbing individuals to test whether they have Covid-19, and for a subset of 10% we are also undertaking antibody testing to work out who might have had the disease.

Alongside that, we set up a number of bits of information to monitor the social and economic impacts of the pandemic. First, we set up a business impacts of Covid-19 study. It reports every fortnight on the impact on businesses—whether they are temporarily paused, the number of staff furloughed and home-working arrangements. There is also an opinion and lifestyle survey, which carries out weekly monitoring. Over the weekend, it monitors compliance with the latest guidance in each of the nations of Great Britain. As we know, compliance with the social distancing measures is an essential part of understanding and controlling the pandemic, and the high levels of compliance seen there are very important. The final part was utilising publicly available data to research people's movements when tighter travel restrictions were in place.

We have worked in partnership with universities, such as the University of Oxford, on some of our data. We make sure that all our data is available only for research purposes and that the individuals are not identified through the use of our survey data.

Viscount Ridley: Perhaps I could ask Mr Whittall to summarise what he would see as the main ethical and privacy concerns around data that have arisen or are going to arise.

Hugh Whittall: We have just heard from my two colleagues that the kinds of data collected are quite broad and vast, covering health status, infection status, antibody status and contact between individuals. So a range of data on individuals will potentially be gathered. Privacy would certainly be one concern, but in a sense the key issue is identifying the context in which data is collected and the ways in which it then comes to be shared and used—whether this is sufficiently clear to the people whose data is being used and whether the whole system is transparent, so that there is clarity of purpose in the data and the apps relating to it. So although people might not necessarily have an understanding of its possible uses in fine-grain detail, they will have had an opportunity to contribute.

There are also questions about time limits and extended functions. The privacy element is not simply in direct conflict with the potential uses of the data; it is important to recognise that it is a little more complex than that. I, as an individual, have an interest in my privacy being protected, but I also have an interest in data that relates to me being used for the public good. Similarly, the public have an interest in protecting privacy, so there is a kind of joint interest here.

There is a concern about the protection of privacy, but individuals will also be concerned to know—it will be an ethical concern—that the data collected for that purpose is used effectively for that purpose. We need to see this in a round context.

Viscount Ridley: To pose your question back to you, is there sufficient clarity of purpose at the moment?

Hugh Whittall: There probably has not been. It is not evident that there has been a gathering of understanding of what people might expect their data to be used for and of the kinds of values and priorities they might have. Listening to the evidence up till now, nor is it necessarily understood which data will be gathered in which context and how it might be combined.

Therefore, I think there is probably work to be done both in involving the public in the design, preparation and management of the systems and in explaining how it will be played out, and how those two things will be governed so as to secure a correspondence between expectations and actions.

Q134 **Baroness Rock:** I would like to come on to the test and trace system that is currently being used. Dr Veale just mentioned some of the advantages and disadvantages of a centralised versus a decentralised system. Who has access to the test and trace data in its current form, and what is it being used for beyond the direct tracing of contacts?

Then, if I may, I would like to come back to a discussion about local targeted action. Perhaps, Dr Veale, you could start.

Dr Michael Veale: I am not an expert on the manual test and trace system, but I can talk about the app side. However, one thing that I would highlight is that the word "decentralisation" is used differently in manual test and trace from the way it is used when we talk about the architecture of an app. When talking about the architecture of an app, the term means that data never leaves an individual's device. It does not mean, for example, that an employer cannot ask for that data as proof of identity as you enter a building or that someone cannot requisition it coercively, but it does mean that the data is not centralised.

The difference in its use in a manual test and trace system is that it implies that local authorities have either access to the data or some say in how it is collected, but that usually relates to a different form of data. I just want to highlight that, but I cannot speak about the on-the-ground situation in manual test and trace in the UK.

Baroness Rock: Thank you. Mr Bell, perhaps you would like to add something.

Iain Bell: I am not an expert. DHSC—the Department for Health and Social Care—runs the data system. We have worked in partnership with Baroness Harding's side to make sure that there is now a weekly publication of test and trace statistics, so public information is available. The Department of Health and Social Care has worked to make sure that that is now available down to local authority level and on a weekly basis.

My understanding is that that data is available to local health practitioners as well. For further uses, the department, which has access to and control of that data set, would have be asked.

Baroness Rock: Thank you very much. Mr Whittall, Baroness Harding talked about local targeted action. We have heard concerns about it not being shared enough. Is there a way in which data sharing can be put through in a fast request without having implications for data privacy?

Hugh Whittall: First, you touched on the question of centralised and decentralised systems. In a sense, that is a technical question of security and efficacy. If the point is to ensure that people who need access to the data get it, and get it rapidly, that could be done through the system—again, it becomes a technical question—but it becoming available to those who, let us say, need it more locally to carry out local and manual contacting is obviously an important function of the system more broadly.

Concerns have been expressed about privacy or confidentiality being an impediment to that. For me, the main point is that that would be because the system has not been designed well enough to account for privacy and confidentiality. To go back to the same point once again, if people are involved in the design of it, those would be their expectations—that the system delivers precisely the kind of protections that other services can deliver. If my data and information go into that system, I would expect that to be built in, both to protect the data from going to my neighbour or my supermarket and to ensure that it goes to the place where it will be used effectively for the purpose that we agreed it would be taken.

Q135 **Baroness Sheehan:** What are the ethical implications of widespread antibody testing for the purpose of providing certifications of immunity? Are there groups that would be more or less advantaged by such certifications? Could there be unintended consequences of pursing immunity certification policies or immunity passports, if you like, either in the public sphere or private context? Mr Whittall, would you like to start?

Hugh Whittall: Yes, I thought you might come to me. We at the Nuffield Council on Bioethics published a briefing note very recently on immunity testing and certification. It becomes more complex, because it is not just about antibody testing. Antibody testing is not yet terribly effective; the testing itself is not clear how effective it is, and numerous tests are being developed. Also, we are not sure how much protection having antibodies has and for what duration, so for the time being we are probably not ready to contemplate that in any event.

However, antibody testing alone is not the whole story when it comes to people’s risk profiles. We have already learned about how monitoring people’s contacts may also contribute to their risk profile. Them belonging to certain groups, whether cultural or social, may also have an effect of their risk profile.

If we start to build the prospect of immunity passports, where all those factors can feed in, we absolutely see the prospect of discrimination, disadvantage and stigmatisation arising from that. That may be people who have positive antibody tests or have a low-risk profile then getting access to employment or services that other people might not have access to.

At the same time, you double the impact on the people who are already subject to structural disadvantage for any of those reasons—social, economic, employment, BAME status, et cetera—and who are at elevated risk from Covid-19 altogether once you start to impose a certification system where, once again, some people might have privileged access to goods, services or employment. Many elements of immunity certification would need to be explored quite carefully before the Government went ahead.

This is not just about the state introducing its own certification system; what might be even more concerning would be if we had private and commercial organisations applying informal certification systems, in effect, whereby people needed to have a private test for immunity to gain access to private commercial spaces. So it is not simply a question of whether the Government should introduce it but of how the Government might think about it when other people might also introduce equivalent systems.

Dr Michael Veale: Before World War I, we did not really have passports. They typically emerged during World War I, and the Spanish flu that followed made them stick around. They were going to be a temporary measure. You can look at the documents from that time and see the narrative change. As for anything that we introduce now, pandemics tend to entrench the infrastructure that we build.

In the discussion on immunity certificates, we see a range of companies that see this as an opportunity to sell a more general-purpose identity system, perhaps relating to health or technology on your phone more broadly, swarming into the government sector. We have to be aware that the choices we make on immunity certification may stick around. Therefore, decisions on it must be subject to extra scrutiny.

The other challenges that relate to marginalised groups in society are also emphasised when we look at the UK legal framework in comparison both to proposed amendments and to legal frameworks in other countries. Other countries that have introduced apps for contact tracing, such as Australia, Switzerland and Austria, have also put provisions into their law saying that such an app cannot be a requirement for, say, access to a normally publicly accessible space or the provision of goods and services: that is, no private person or legal person can require that an app is presented as a prerequisite to that. A similar Bill in the UK was proposed by academics, including me, and led by Professor Lilian Edwards, saying that a similar provision has not been put in place.

Lastly, any app or immunity certificate, or anything of that type, will indicate something about health. Health is not a protected characteristic under the Equality Act. That creates some challenges. It could be used as a proxy for discrimination in areas such as immigration, employment and housing, particularly as we do not know how long coronavirus will stick around. That is something to be very wary of; such technology or documentation could be used as a means for arbitrary refusal to particular groups, for example in line with immigration policy.

Baroness Sheehan: Excellent. Thank you very much. I have a small supplementary question. I think I know the answer to it, but perhaps the witnesses can confirm it. Is there any likelihood of behaviour changing if there is an immunity passport? Would it incentivise people to contract the virus?

Hugh Whittall: It is difficult to say, because we have not been through this process before. It is a novel situation. One can certainly see the reasons why some people might do that. For example, people in low-paid and precarious employment may not be able to work if they do not have an immunity certificate. They may face a simply impossible choice: either they expose themselves to high levels of risk in yet more precarious employment or they expose themselves to the risk of infection in order to get the certification. Certainly, that would be a concern.

As I said, we probably need to do a fair amount of work to understand people's motivations and the kinds of risks that they are willing to take in those situations.

The Chair: I get the message that on the whole you think the immunity passport was a bad idea.

Hugh Whittall: I certainly think that the case for it is far from being made at the moment.

The Chair: Let us go back to the previous question about data collection. Who should have access to this data?

Dr Michael Veale: It obviously depends on the purpose. When I and the University of Oxford but primarily EPFL and ETH Zurich, the two major technical universities in Switzerland, were developing the decentralised contact tracing system that is now used in Germany, Switzerland and many other countries and is on everyone's phones based on Apple and Google updates, we started by asking: what do we want to achieve? We worked with epidemiologists and asked them what they needed from a contact tracing system that uses Bluetooth. Then we asked: what do you need from the data? Using cutting-edge privacy technologies to achieve it, what is the minimum amount of data transfer that you need?

In this case, nobody needs access to the data. All you need is one person who has been diagnosed and the telephone of another person who recognises that they are at risk. They can then send that information to a public health authority and can be called or given a pop-up. If you cannot avoid the middle creation of a network of society that is unnecessary and, according to our epidemiologists, not particularly useful operationally because Bluetooth is not a very high-quality technology for establishing that kind of data, we should not collect it because we want to maximise trust.

Therefore, sometimes the answer technically is that nobody needs the data, but in other cases the answer should always be based on need. If possible, data should be aggregated, but sometimes that will not be applicable. So there should be careful consideration of what the evidence says is needed at every level in order to ensure maximum trust.

Furthermore, data should not be retained. There is a risk that some academics in epidemiology will see this as a chance to gather a data trove for analysis which PhD students can work on for years and years in advance. If that comes at the cost of public trust in, and thus the success of, these schemes, we must push back against that. We have to take those questions very seriously and have that discussion in public.

Baroness Walmsley: Mr Whittall, in response to Viscount Ridley a few minutes ago, we heard you give an outline of the sorts of data, privacy and security concerns that there are about contact tracing apps. Do you think that decentralised approaches can overcome some of those concerns, and, if so, how?

We have also heard that these apps can collect many different kinds of data for lots of different reasons. I would be interested to know what you think the minimum data is that needs to be collected for the primary goal of reducing transmission. From what he has just said, I think that Dr Veale might want to come in on that part of the question.

Hugh Whittall: I am not sure that I can reach a view on whether centralised or localised systems will be more functional. That is probably too much of a technical question for me. One would be concerned about ensuring that the data collected is only that which is necessary for the intended purpose. If the intended purpose is simply to be able to identify contacts, that is a relatively small amount of data, which can be channelled through a centralised or localised system.

I do not know which of the two is better, but ultimately it needs to arrive locally so that it can be used by those who need to do the contact tracing. I think we are learning that it is better conducted by people who have better local knowledge. If we look at that within the context of a wider system of conducting appropriate surveillance of disease transmission to inform understanding for the future and how that will work, there are probably other types of data that may be useful.

There are some important principles here. One can go back to the foundations of the Data Protection Act, which is about the fair, lawful and transparent use of data only for the purpose intended. If we keep those principles in mind, we see that we should not hoover up as much data as possible simply so that we can have more of it. Nor should we extend into the future the uses beyond those that were originally intended, or keep data for longer than is necessary for the specified purpose.

If people are invited to participate in the design of these systems so that we have a good understanding of what they expect them to deliver and we involve them in the oversight of that—not everybody individually and not with individualised consent but in broad terms—and if we can understand those expectations and deliver them, and not extend the purposes, it is quite possible to construct a system that can meet all that.

However, I am sorry to say that at the moment I do not think that there is enough transparency about how the system is being constructed, operated and governed for us to have complete confidence in it.

Baroness Walmsley: Thank you. You just mentioned information going to local people, such as directors of public health in local authorities. We have heard from some witnesses that it has not been reaching them in the right form or in a timely way, or indeed with sufficient granularity. Can you suggest what can be done in the future to make sure that the right information gets to the people who need it in local areas in a timely way?

Hugh Whittall: The technical means by which that is done are manageable, but the difficulty is that from the outset there was no shared understanding of who would need access to the information and for what purposes. It seems to me that that prior discussion was not had; nor was there transparency over the agreement about who would receive the information, who it would be shared with and for what purposes. My reading of it is that we have run into a block, because from the outset there was not sufficiently strong shared understanding. It is not a technical question.

Dr Michael Veale: Perhaps I can add a small amount on the original question about what data would be required. This adds a little to what the witnesses in the previous session—neither of whom, I think, were in their positions at the time—said about some of the motivators behind the choices that were made a little earlier in the app development.

The United Kingdom, unlike every other country that we were working with and which were developing apps at a similar time, did not have a speedy testing facility. It was not able to say reliably that tests could be returned within 24 hours for everyone in the country. That data is very important for an app to function; you need reliable data about whether people are truly positive so that you are triggering people and they will retain trust.

That caused challenges for privacy and trust early on, because it led the UK down the route of wishing to construct a centralised system based on self-reporting, which other countries were not doing. Indeed, the French Minister, who also uses a centralised system for a different reason, said that that was out of the question for France. It just was not on the table for other countries, because hypochondriacs and people who wish to misuse the system could trigger false alerts. So it led to a bit of a challenge here. It emphasises that many of these interventions and the data on them are heavily interlinked. The design of an app that is trustworthy and uses only the minimal data requires a fast testing system to exist.

Otherwise, my colleagues and I in our projects, and I believe many academics around the world, would say, "Do not use an app at that point; you have other problems to deal with before that intervention has a chance of success".

We will see whether they work to control the virus. These are of course experiments and it is still early days for everyone, even the countries that have significant penetration already.

Baroness Walmsley: Thank you. Did I understand you to say earlier that, for the primary purpose of reducing transmission, all you need is the phone number of the primary case and then, going on from there, the phone numbers of the contacts?

Dr Michael Veale: There are two points there. That is what you need—actually, you do not even need the phone numbers—to trigger an alert among the other individuals. The question is whether you want them to be called. If you want them to be called, they will have had to input their phone number in the app at some point. That can be sent in a private way that does not disclose the social network of the whole country, which is the important data risk that we are trying to protect against. In terms of efficacy, we are still learning about what will make people trust the results of an app, if indeed they will. We have not evaluated this.

The Prime Minister said recently that no country has a functional app. There is a lot to unpack in that statement. No country has a functional app in the sense that there has not been a retrospective peer-reviewed study six months on, because six months have not passed. But many countries have apps which they believe work functionally to a high degree with Bluetooth. Bear in mind that the UK was planning to roll out the app used on the Isle of Wight on self-reported symptoms, the reliability of which would have been heavily questionable and much more of a problem than worrying about whether it would do 1.5 metres or 2 metres reliably.

We are waiting to see. Monitoring and evaluation will be key to gain trust and to learn for the future.

Baroness Walmsley: Do you think that here in the UK the current regulations are sufficient to ensure that people’s data is protected? Is there really a risk that these protections could be overlooked because we are in an emergency?

Dr Michael Veale: There is certainly a risk that they could be overlooked. There are many aspects of data protection law covering areas such as automated decision-making. However, there are perhaps two more important points.

First, we must look beyond privacy to power: to coercing people to use this app and get services in response to it. That is the main area where regulations are lacking in the United Kingdom.

Secondly, the other area that needs to be considered is interoperability with other countries. It is key that these apps work together across countries. You cannot swap at the border; for tourists and the like coming in, the past and future history needs to be fluid. In that case, we need an app that works well internationally. Decentralised apps not only work well together, unlike combining the two, but it is a bit of a zero-sum game: people choose one or the other. If you all end up choosing a centralised app, you are encouraging Hungary and Poland to have a centralised app, and there are human rights implications to that. Those are all important aspects to consider, and the regulatory landscape needs improvement in those areas.

It is worth noting that Northern Ireland has already finished development of a decentralised app, using the Republic of Ireland code, and that Gibraltar has already rolled one out. We are talking here about the English app; NHSX is linked to NHS England, and the other regions have different technology projects at different stages of development.

Baroness Walmsley: So looking forward to the Apple/Google technologies, and the app we are expecting, and given what you have just said about self-reporting apps, do you think that the new app will avoid the security and privacy concerns you identified with the earlier version of the app?

Dr Michael Veale: Yes, I believe that it will avoid the security and privacy concerns of the earlier version. People discuss the Apple and Google system, but interestingly it was based on research, including from my group and others in the UK, working together with other countries, which convinced the companies to develop it in this particular way.

We believe that it is a much more trustworthy system from the point of view of privacy and preventing function creep. A big concern was that this could turn into a quarantine control system. The initial NHSX proposal, which was similar to ideas proposed in many countries around the world, could be extended trivially—just by putting sensors in railway stations or supermarkets—into a quarantine control system, where you can monitor whether or not somebody has visited a certain place.

We were concerned about that function creep in many countries. I am not thinking of the UK, which obviously has a robust regulatory regime in these areas. But we were developing for the world and were very conscious that this is a time of emergency powers—Hungary, for example, has suspended all Covid-related data protection provisions—and there is a need for technological assurance and reliability.

The Chair: We can come back to this, but I want to bring in Lord Winston.

Q136 **Lord Winston:** Thank you. I apologise; I have to leave for another meeting. However, I would like to start the ball rolling, and perhaps the Chair, or Baroness Rock or Baroness Blackwood, might like to follow up on it.

How are the Government meeting their requirement to make an assessment of the ethical and privacy values of the pandemic disaster? I am thinking in particular of the problems in the health service, where there is huge difficulty getting people tested and with what happens to the results of those who have had to be tested and so on.

Forgive me for leaving now, but I shall read the transcript of the rest of the proceedings with great interest.

The Chair: Someone’s mic is on. Please can they mute it? We can hear a lot of background noise.

Iain Bell: At the start of the Covid-19 pandemic, the Office for National Statistics ensured that all our data collections went through our National Statistician’s Data Ethics Advisory Committee. That ensures that everything that we do is underpinned by sound ethical principles and governance to ensure that it is set up correctly.

In addition, for the infection study we set up, we paid particular attention to the ethics proposals. For medical ethics, we went to the University of Oxford’s ethics committee and included data ethics on who could and should access the data. Picking up the points made earlier, part of that is to ensure that the project is in the public good and accessed only for legitimate purposes of research in a safe setting. That helps to provide that strong governance over our system to make sure that the transparency is there.

Turning particularly to patients' data and access to the test results, we have only anonymised access to the data, so we never know which individuals have tested positive. Through the GP, we notify the individual that they have had a positive test in order to ensure that they have that vital information. Under the pandemic measures, the GP is required to make sure that Test and Trace is notified. All this has gone through the university's medical research committee and is in line with standard practice. The National Statistician's Data Ethics Advisory Committee is available for use across government in order to try to bring about ethical guidance and control.

Those are the procedures that ONS has put in place to manage this.

Hugh Whittall: I should say that my remarks do not refer specifically to the committees of ONS but rather to broader questions of government policy, partly as it relates to the use of data and the app, and more broadly as it relates to other elements related to the management of the Covid-19 crisis.

One of the difficulties here, which Lord Winston asked about, is whether the Government have made adequate ongoing assessments of ethical considerations. The difficulty is that we do not really know. In the past, we have said explicitly that we would like to see more transparency, not just on the background science on which the Government are taking advice but on the values that are being used to exercise judgment, because decisions are never led entirely by the science.

There are whole parts of the process—who government engages with and where there are opportunities for diverse voices to contribute to discussions—where transparency is needed about the kind of engagement taking place and the justification for decisions that are made, whether it is about the app or other things.

We are aware that the Moral and Ethical Advisory Group, which was established last year, has had some meetings, but that seems to have made a rather marginal contribution to the decision-making and considerations here. An ethical advisory group was established to support the development of the app. It is not clear, but we think it has probably been stood down now as we have now moved on to a different system. I remind your Lordships of the letter that Jonathan Montgomery, the chair of that committee, wrote to the Prime Minister outlining the importance of these things and the value of what is being done—in fact, to establish that it will have the effect that is intended: security.

Then we have accountability, transparency and the control that people will have of the use of their data. In response to the question that was put, I do not think we have a clear sight of the involvement of public voices, the transparency of decision-making, the values that are being used and in what way, and how ongoing governance arrangements will be in place to secure that continued involvement and oversight.

That is in very broad terms, but, as I say, this applies to rather more than simply data use in this context.

Baroness Young of Old Scone: Before I go on to my questions, I want to ask Iain Bell about the best practice and impact service. You listed in your evidence that it has covered test and trace and PPE. Are there issues of data in this crisis that you would dearly like to give advice on but have not yet?

Iain Bell: No. At this point, I feel adequately consulted on providing advice to the Department of Health and Social Care. It knows that, whenever it needs any advice from us, it only has to pick up the phone. At this point in time, I am comfortable that we have worked well together in order to improve and put out the statistics on test and trace and PPE.

Baroness Young of Old Scone: So there are no areas that you feel you ought to have been involved in and you have not been?

Iain Bell: No, not at this stage. There are areas where we work in partnership to identify potential gaps in the data, so things that are likely to come up as being future questions. At the moment, for example, we have studies that look at the prevalence of Covid-19 in care homes and community settings. Are there other settings where we should be working in order to get a better feeling on transmission? Could we, for example, look into airports? I work in partnership with colleagues across government to identity those gaps and put suggestions forward for filling them.

Q137 **Baroness Young of Old Scone:** Thank you. I turn to Mr Whittall, who talked about diverse voices. I want to explore the business of vulnerable groups and their particularly challenges in terms of privacy and the use of data. One example is homeless people. Could you give us a feel for what you would regard as the most vulnerable groups? Is data being collected on the basis of these groups, and are they being adequately brought into the process that you have described as being an integral part of how systems are devised in order that they understand what is happening?

Hugh Whittall: I do not know in any level of detail to what extent data is being collected or what types of data are being collected. Others may have that information. To step back a little, vulnerable groups, who may be homeless people, or undocumented migrants, are not well served by excluding them from data collection, because we have to understand impacts, where the opportunities are perhaps to provide services and to ensure that protections are in place.

Of course, there are potential risks and anxieties that those people may have about engaging with people who are collecting data, especially those who feel that that information might be shared with other authorities. It is important to include vulnerable groups but at the same time to have secure, well-governed systems in place that can give them assurances that they should not be anxious and should not lose trust in the system because of a fear that that data might be going to places that they had not intended it to go.

Again, I cannot speak for what is happening on the ground in this context, partly because again I am not sure—others may correct me—that it is as transparent as that that we know that information.

Baroness Young of Old Scone: Mr Veale, do you want to comment on whether data is being sub-sorted by vulnerable groups? Is there identifiable data about some of these groups and are they being sufficiently informed about what is happening with that data?

Dr Michael Veale: I have not seen evidence of that in the UK, but it is something that we have seen regularly in other sectors and it forms a consistent risk.

One interesting point that I would note about vulnerability in the context of Covid-19 and in relation to an app is that the people who are most vulnerable to Covid-19 are the ones who least need the app, because if it gets to them it is already too late. The app is for protecting others, not yourself. It is about alerting people whom you have been in contact with, so the elderly and the shielding do not necessarily need an app as much as the people who would visit them do, because you do not want them ever to get to the point of visiting them, if you see what I mean. That is the point of shielding.

It is just an interesting dynamic when people point to that. Of course, when we think of marginalised and vulnerable people we are not just thinking of those who are clinically vulnerable.

Hugh Whittall: I want to add one thing, if I may. If you look at this in the context of the prospect of some form of immunity certification or risk profiling, once again those who are more vulnerable—not simply those who are homeless, undocumented or outside the systems but even those within the systems who have precarious existences, such as people on zero-hours contracts—simply have no leverage with potential employers.

So once again, the potential uses of data in those private contexts could leave people who are already vulnerable yet more vulnerable because of the relationship between them and the systems that we operate under.

Q138 **Baroness Blackwood of North Oxford:** We have focused a lot—absolutely correctly—on the risks and challenges of data collection in manual contact tracing and the app. That is completely appropriate. I presume that there is also agreement that there is value in using this data in an appropriate manner, not just for public safety but hopefully for ensuring that we are prepared for whatever may come next in research and clinical understanding.

I want to focus on what we can do to make sure that that data is used appropriately and how we can ensure that there is public trust and confidence in the way that data is used. In other words, how can the Government get this right, and how can the private sector get this right when it is working in partnership?

Perhaps we can start with you, Dr Veale. What would be your recommendation for how the Government can ethically and appropriately gather this data? What should they do first?

Dr Michael Veale: There are different levels. One thing we can do is ensure that we put privacy and ethics first by developing tools that provide value while also securing privacy and ethics. Those tools can be designed in advance of a pandemic. It is what we try to do with our project here.

Procedurally, you can be more open about the private companies that are being worked with. There is considerable concern in civil society that the UK Government have been making effectively commercial arrangements with private companies that have a long-term interest in data access, building the infrastructure and locking in services to a particular proprietary closed system that they can monetise later on, and they are doing it as a very cheap pro bono thing at this crisis stage.

To combat that, you need capacity in the public sector to understand when you are being played by a private company. You need transparency about contracts. You need open standards to say that you are not permitted to purchase or enter into arrangements that lock you in technically to certain standards or computational systems, because any contractor is obliged to leave the pathway open for someone else to take on the work going forward without using their intellectual property to do so. This is not difficult, because all the best analytic tools of the trade are open source, which means that they are freely available for anyone to use. Google, for example, relies internally solely on analysis using open source tools—that is its bread and butter—so we can do this too.

We need these types of arrangements in the long term. We may also need to think about building a register of the analysis that is being undertaken and the analytic systems that are being used, particularly as these systems become more advanced or have the possibility of entering operational use rather than just research use. Accountability on those is proper.

Lastly, the publishing of data protection impact assessments is critical. We have not seen that happen; indeed, it appears that NHS England has not carried out data protection impact assessments for all of its test and trace system, and it has definitely has not published them. This would be very good practice. Ideally, it would be on a statutory footing that in certain sectors such impact assessments are required to be published when they are made.

Hugh Whittall: First, I completely agree. We absolutely recognise the benefits that can accrue from harnessing data for public good and seeing that it is not intrinsically in conflict with potential private concerns. As a private citizen and a member of society, my interest is in both privacy and the deployment of data for public good.

Going forward, it is really important that we think from the outset about involving people. I talked earlier about diverse voices. If we are to have systems that are consistent with people’s interests and values, we must identify those interests and values by talking to people and understanding what they are. We have to engage and involve people at all stages of that process.

I will come back to that, because it can then, from the outset, be built into both public and private initiatives for data collection and use. Such initiatives must be transparent about what data they will gather, from where and in what context, as well as about who will get access to it and for what purposes. That can be publicly declared. Too often, transfer data arrangements are not published. We need to have better transparency here so that we have governance systems that can oversee that.

Once again, coming back to the inclusion point, these governance systems can include people from civil society who understand, recognise and see that those public interests and values are consistently applied throughout that system. This is not about simply sticking to the law. We can do that, but we can also do better than that. In these systems, what will eventually generate and maintain public trust is that, when such a system that will be for public good is declared, do it; deliver the good that it says it will deliver and do not do other stuff.

Baroness Blackwood of North Oxford: Yes. Say what you are going to do, explain the benefit and then deliver it effectively. I presume also that, in setting up a project, it is possible to have layers of consent to allow for the fact that many people out there will be very keen to support the Covid research effort and may well want to donate their data, but that there will be others who have a different privacy threshold and are not comfortable doing that.

It is about providing a transparent consent process so that people understand what data usage they are consenting to. Some people might consent to their data being used for research but others might say, "No, I'm not content with that. I just want it to be used specifically for contact tracing in my personal situation". That is a perfectly ethical and appropriate process to use.

Hugh Whittall: I agree. Can I just dwell on the consent question for a moment? Consent is important. There are some circumstances when absolutely specific consent is required, for example in medical situations. There are others where—here, the data context becomes more complex—it is difficult sometimes to specify precisely what purposes data will be used for. So we must accept the notion that some consent is broadly expressed.

Different governance systems can exercise different levels of control over that. Some people may decline and stay out of it, which is fine. But there are other circumstances, and public health is one of them, where we do not need consent. For infectious disease that is absolutely deadly, for example, there may be circumstances in which data is gathered at a fine-grained level and we do not need to seek consent. If that is the case, other parts of the ethical infrastructure must serve the purpose of governing, overseeing and reassuring us that the data is still being used only for the legitimate purpose for which it is intended.

Consent is critical, but other parts of the system also deliver those kinds of ethical assurances where consent has a more limited role to play.

Baroness Blackwood of North Oxford: Iain Bell, do you want to come in on any of these points? I am conscious that we are coming close to the end.

Iain Bell: Mr Whittall is absolutely right. The core of this is being explicit and up front about the purpose of the data being collected but accepting that sometimes there is broad consent. In our Covid-19 infection study, for example, participants had already agreed that they were happy to be contacted for future research without it necessarily being stated whether that would be to do with labour market fails or other factors.

That ethical framework kicks in because broad consent is really important. In some studies, if you only go with the people who give consent, you may not truly understand the course of the pandemic, so sometimes you need that broad overview, within the consent given and never overriding that, to make sure that where you have consent you understand the characteristics of those who have given consent and those who have not so that you can truly monitor the pandemic and its impact.

Q139 **Baroness Manningham-Buller:** Dr Veale, you gave us a very clear description of the development of apps and the fact that some are obviously experimental. Is there a country or set of countries whose apps you would point to as exemplars of getting the balance right: that is, getting the information you need without any danger of coerciveness, or creep as you put it? Are there any people we should look to?

Dr Michael Veale: Yes, certainly. That exact balance was at the centre of the design of our DP-3T system, which has gone on to completely underpin the work on the app in Switzerland; it has been ready for quite some time, but the parliament spent a long time making a preparatory law to accompany it, so it was delayed for a while. Then there is Germany, where the app is very well engineered and has been rolled out widely across the country. I would also look to the work done in the Republic of Ireland, which not only opened up its source code but donated it to Northern Ireland and Gibraltar, which have both developed and rolled out apps on the basis of that.

Baroness Manningham-Buller: Good. You had mentioned them already. Anywhere else?

Dr Michael Veale: In terms of the exemplars? No. Other countries have used the system, but the situation in Switzerland is a great exemplar, because it involved its core universities and civil society widely from the beginning; it has also had debates in parliament to hash it out. Germany, too, has had a good level of public discourse from the beginning and changed versions of the app that it used in response to public discussions. That was early in April, whereas the UK took a long time to get to its conclusions.

I would look at the processes there and who they involved, as well as how regulators were involved in the data protection impact assessments that were used. They are much more substantive than the documents that have been produced in the United Kingdom.

The Chair: Thank you very much. I am sorry that I lost my connection for a bit. I had technological problems. I do not know why that happened. I cannot wait to get back round a horseshoe-shaped table, but there we are. I thank Dr Veale, Mr Whittall and Mr Bell for coming to help us today. It has been most interesting to hear you. Thank you for making time to do this. We will close the session now.