HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Harnessing the potential of new digital forms of identification, HC 986

Tuesday 18 November 2025

Ordered by the House of Commons to be published on 18 November 2025.

Watch the meeting

Members present: Dame Karen Bradley (Chair); Lewis Atkinson; Margaret Mullane; Chris Murray; Peter Prinsley; Joani Reid.

Science, Innovation and Technology Committee member present: Dame Chi Onwurah.

Questions 1 - 57

Witnesses

I: Laura Foster, Associate Director, Tech and Innovation, techUK; Alexander Iosad, Director of Government Innovation, Tony Blair Institute; and Professor Edgar Whitley, Professor in Practice (Information Systems), London School of Economics.

II: James Baker, Programme Manager, Open Rights Group; Silkie Carlo, Director, Big Brother Watch; and Ruth Ehrlich, Head of Policy and Campaigns, Liberty.

Examination of witnesses

Witnesses: Laura Foster, Alexander Iosad and Professor Edgar Whitley.

Q1 **Chair:** I welcome the witnesses to the first oral evidence session of our inquiry on harnessing the potential benefits of digital identification in the work of the Home Office. Before I ask the witnesses to introduce themselves, I am just going to make an opening statement.

I want to acknowledge the level of public interest in this inquiry. We have received more than 3,500 written evidence submissions, with most coming from ordinary members of the public. That was even before the Government announced their plans for digital ID. The vast majority of submissions from individuals were strongly opposed to mandatory digital ID.

The role of this inquiry is not to decide whether or not mandatory digital ID should be introduced, but to examine the strength of the evidence for and against digital ID, particularly in the areas of crime and immigration, and to scrutinise the Government's policy on making digital ID mandatory for right-to-work checks by the end of this Parliament.

We will carefully consider the views of those members of the public who have submitted evidence, as well as of our own constituents, alongside the views of our expert witnesses.

Can I ask the witnesses to introduce themselves?

Professor Whitley: I am Edgar Whitley. I am a professor of information systems at the London School of Economics. I have spent 20-plus years studying digital identity in the UK and globally. Particularly in the context of this inquiry, I have also been supporting and working with both DSIT and GDS for the digital identity and attributes trust framework and for One Login as well.

Laura Foster: Good afternoon, everyone. Thank you for inviting me to give evidence today. My name is Laura Foster, and I am the associate director for tech and innovation at techUK. If you are not aware, techUK is the UK's tech trade association. It is our job to represent the UK tech sector and showcase how technologies, when they are applied in an ethical and responsible way, can have a positive impact on UK society, the economy and the planet. Through our digital ID working group, we are the industry voice for digital ID. We host events and webinars and publish a lot of policy thought leadership. Most recently, our digital ID report came out in October; it was the first industry response following the announcements from Government.

Alexander Iosad: My name is Alexander Iosad. I am director of government innovation policy at the Tony Blair Institute. Thank you very much for inviting me today. The Tony Blair Institute is a non-profit that operates globally in more than 45 countries, advising political leaders on

strategy, policy and delivery. In the UK, we operate essentially as a think-tank and as a policy research institute. We do research, we talk to people, we publish papers and then we hope that the ideas we put down are picked up by a Government of the day.

I lead a team that is focused on public service transformation. It is a global team—we cover both the UK and global policy, and we hope to blend that expertise across borders. We have advocated strongly for a form of digital ID to improve public services in the UK for more than five years at TBI.

Chair: I welcome Dame Chi Onwurah, Chair of the Science, Innovation and Technology Committee. She is guesting on the panel today because her Committee also has an interest in this area and we want to ensure cross-Committee working.

We will go into questions, starting with Peter Prinsley.

Q2 **Peter Prinsley:** My first question is very wide, and you could probably spend all afternoon answering it. We would like to know what you see as the main potential benefits of a more widespread adoption of a digital form of identification in this country.

Professor Whitley: Digital ID, per se, has lots of advantages. For me, the big question is always how you implement it, but the idea is that you have a digital credential that includes facts about yourself—attributes, particularly; the identity part is less important. It is mostly the attributes—that come from a source that is the appropriate source to give that attribute. So, my university is the best place to determine whether you have a degree from that university; the UK Government is the best place to determine whether you are a citizen, and so on.

The idea of having a digital representation of identity, and particularly attributes, is definitely a useful thing, because it takes all of those different documents that are typically used to prove those claims and puts them in a form that you can use and share. The big question, of course, is how you go about doing that, but there will probably be a later question on that.

Laura Foster: I will start by talking about the economic benefits of the digital ID sector to complement what has already been said. In case you are not aware, the UK already has a thriving digital verification services sector. They employ over 11,000 people and deliver a £2 billion impact to the UK economy—a figure that is set to double by 2030. Those companies are already delivering services to millions of citizens who have chosen to use digital ID, and the benefits in the cases in which they have chosen to be used are great.

They can be used for a teenager or a young person who wants to access their academic record. They can be used for a retiree who wants to verify that they have a right to access their pension. But actually, where we see most people already choosing to use digital ID is in the financial services industry and for fraud mitigation. Why is that the case? Well, digital ID

allows the presenting of trustworthy information so that it can help streamline services and reduce compliance costs. For the financial sector, digital ID is already delivering benefits.

I will finish by saying that the financial sector sees the compliance benefits of digital ID as really important, but, through the Government's own statistics, time savings and convenience are the reasons why citizens are choosing to turn to digital ID to access services.

Alexander Iosad: I agree with everything that my co-panellists have said. From a public services perspective, when we talk about digital ID, we talk about the ability to prove that you are who you say you are, and that is an identity element. We talk about the ability to prove that certain things about you are true. Again, with digital identity, that can be done much more easily in a much more convenient, private and secure way.

We also talk about the ability to access services on the basis of who you are and what we know to be true about you, and that opens really exciting possibilities for how public services, and services more broadly, operate. It allows us to move from a reactive, one-size-fits-all model that was built for a different age, to a personalised, preventive model with a layer of accessibility that is not possible with a traditional model, where you have to apply for every service and prove again and again things about you that the state may already know.

An additional benefit to digital ID is the ability to change how public services operate to make them much more responsive to citizens, and to put citizens in control of their own data in a way that is not currently available to them. This is something we see countries around the world embark on as a journey, and one where the UK has arguably fallen behind.

Q3 **Peter Prinsley:** You have partially touched on my next question, which is about the impact that the widespread adoption of digital ID could have on crime reduction and particularly on fraud.

Professor Whitley: Crime reduction is a very broad concept. It will not have that much effect on street crime. You could potentially link the photo that you might have as part of a digital ID to face recognition cameras, but that is a horribly complicated mess. On fraud, as Laura has already said, a key part of the requirement for the financial sector is to know your customer. Everything that you can do to simplify that process will reduce the risk of fraud because the customer is better known. It will not stop all fraud because quite a lot of financial fraud involves, for example, mule accounts, where I am definitely the person who opened the account and definitely a real person, but I am using my account for fraudulent transactions and getting a payment for doing that.

It will not be a panacea, but for the initial registering of an account—making sure it is a real person, and so on—it has an important role to play. Bear in mind that the onboarding of customers is not just the "know your customer" anti-money laundering checks; there are a whole lot of

other, "What other services and products can we sell to you?" offers. It is also not going to fix the fact that everyone can have a bank account in 10 seconds.

Laura Foster: Just as crime can be an incredibly broad term, fraud can be incredibly broad. There are different types of fraud. Fraud is the UK's most common crime. It is 40% of all crime and costs the UK £6.8 billion every year. Identity fraud costs the UK over £1 billion every year. That is where digital ID probably finds its sweet spot. CFIT has already said that there could be £1.7 billion in savings in compliance and time-saving costs to build on from "know your customer".

Fraud is multifaceted. It is changeable. Digital ID will have to be deployed in a way that does not add to fraud, but it could mitigate fraud. Government are already realising the benefits of digital ID for mitigating fraud. That is why they are currently going through the process of changing anti-money laundering guidance and attaching it to something called the trust framework so that there can be clear guidance on how digital ID can be used within the financial sector. I am happy to talk more about the trust framework.

Q4 **Peter Prinsley:** I want to move on to another thing that is very topical. A lot of people have said that a mandatory digital ID would help with our immigration system. Do you believe that to be the case?

Alexander Iosad: We do not believe that digital ID is a silver bullet for anything, including the reduction of irregular migration. I am sure that we will get into more debate about that.

Where I see an argument for digital ID helping to reduce the pull of the UK for illegal migration is, first, in narrowing the business model of organised criminal groups that are exploiting people to get them across the channel. We know that they advertise, as part of their services, the ability to access falsified documents. They hand you a paper passport that, under current systems, which are quite fragmented when it comes to existing checks such as right-to-work checks, can be essentially waved through with no record of that happening. There are loopholes in the system that a universally used system—we should get into the mandatory element of this in more detail—for digital verification of the right to work can help to close.

A second element is the ability to target enforcement much more accurately. At the moment, we have essentially told businesses that they are responsible for carrying out these checks. We have made it quite hard for law-abiding businesses to carry out their legal obligations and quite easy for those who do not want to follow those rules to slip through the net. With a system that allows us to have a record of which checks are being carried out, we can target enforcement much more accurately.

Q5 **Peter Prinsley:** That answers my next question. There would be some point to this from the point of view of checking whether employers are complying with this stuff.

Professor Whitley: That becomes a boring, technical architecture choice. You are now creating a record—which, the proposals suggest, is shared with the Home Office—of every time my digital ID is checked for a right-to-work check. If you have built in the capability to create an audit trail of those checks, you can easily imagine all the other digital ID checks and see a good, sensible argument for, say, improving the health of the nation by checking every time you prove that you are over 18 if there was an age limit on when you could buy cigarettes, or when you prove your age in order to buy alcohol. Would it be okay to also have an audit trail—a record—of that, not to target enforcement, but to target health interventions? That is where the technical choices, as opposed to the high-level principles, become incredibly important. I suspect that a large number of the individual submissions address an unease at that kind of scope creep.

Q6 **Peter Prinsley:** A surveillance society problem.

Professor Whitley: A record-keeping and auditing society that could then be used for other purposes.

Q7 **Peter Prinsley:** I have two more bits to my questioning. One is about international models. There are plenty of countries where this is happening. What would be a good example that this country could learn from?

Alexander Iosad: I do not think any country has built a system that operates in the way that we think the technology can do and that has got all those technical architecture points right—I completely agree with you that most of these questions are boring technical architecture questions. There are countries that have done different elements well. Countries like Ukraine have kept the data safe and secure, even in the face of really massive cyber-attacks. Countries like Estonia and others have done well on disclosing the data that the state holds on you, who accesses it and for what reason. Countries like India have done remarkably well on the scale of implementation, and in countries like Singapore satisfaction with public services rapidly improved as digital ID was rolled out. For the UK, the opportunity is that of being a late adopter that takes the best of every known implementation to build something that works for us.

Professor Whitley: Just on the India example, because it is frequently pointed to, yes, it has scale, but it is designed only to ensure that every person has a unique ID or, technically, just a number—people laminate the letter with the number on it, because they are still very much a paper-driven economy in large sectors. But it has no attributes about you; it does not even do citizenship. It does residency, because anybody who is resident in India can get an Aadhaar number.

Laura Foster: I agree that there are elements from lots of different nations that we can learn from and draw on here in the UK. I would highlight examples that align closely to the UK, such as Sweden, where the digital ID system started through banking—they have a bank ID. Canada is another example. There are also parts of the eIDAS scheme—

the European scheme—which is a framework setting out what good digital identity looks like.

But I would add two points. We need to recognise the nuances in this country; we are a country with a mixed history when it comes to mandatory or national ID. We need to meet UK citizens—UK populations—where they are and where they feel comfortable with what has already been used. We also need to recognise that the UK already has a marketplace when it comes to digital ID.

I would also comment on something that was just said about the UK being a late adopter. We are not actually a late adopter. The Government's own statistics show that 44% of the people they surveyed have already used some form of digital ID service in the UK. Again, it is primarily for things such as opening a bank account or for right to work or right to rent—through the trust framework, you can already use digital ID for right to work.

Q8 **Peter Prinsley:** Finally, if the Government are to do this for the British people, how do they sell this as politically acceptable? We have received thousands of submissions, most of which, as you correctly predicted, were in opposition to anything remotely like this. I think many of us can see the huge advantages of this system in all matters of state, but how would you go about presenting it simply and understandably to the British people as something that is a big advantage to them?

Professor Whitley: It is interesting—with my academic hat on—that your language has moved from "sell" to "persuade". If this is something that works for people, they will choose to adopt it, because it makes life easier and so on. But we still do not have the perfect model for how this is going to work.

To take a simple example, if you want to do a digital right to work, and you are a freelancer, you could, in an extreme situation, have to prove your right to work with 49 different ID providers, because there are 49 companies, and they have all done a deal with different employers. Then, the 50th time, you have to do exactly the same checks to access your online tax returns. It is great from a market perspective, but it is not quite there yet from a citizen's perspective, which is part of the problem. There is also a lack of clarity on the details of how it will actually be implemented. What choices are being made? What choices are up for consultation? What choices are up for decision? It is very difficult to sell a vision without the detail behind it.

Q9 **Peter Prinsley:** Could you see it being an app, for instance?

Professor Whitley: Realistically, the form of implementation for those who have a smartphone will probably be an app, but that is just the method of delivery. Aeroplane tickets used to be paper, and they are now on a smartphone app, but it is just a representation of the underlying data.

Alexander Iosad: I completely agree. This will be taken up and embraced if it is useful, and that is what we have seen around the world. If people see the benefit, they will look at it and accept it. Even Estonia's introduction of digital ID was met with significant controversy 20 years ago, but we have all forgotten about that because it was so long ago. Because it has proven to be useful, they are now very proud of it. Talk to any Estonian and they will tell you all about it.

What we need to do in this country is to have a very clear vision of what we want to accomplish, and in our view it is about improving public services and the interactions between the state and the citizen, which are so difficult today. And it is about delivering quick wins, so having a very focused delivery plan that is communicated in the open and that allows people to see the progress very quickly.

Q10 **Margaret Mullane:** I want to pick up on what Professor Whitley said in his opening statement, that the Government are the best judge of ID.

Professor Whitley: Certain attributes about you are things that the state issues. I cannot come along and say that I am a citizen of Germany because that is something the German state decides. The British state says that I am a British citizen, and if I were not, it might still say that I have the right to work. It is the idea of a trusted authority that is the correct issuer of attributes that are linked to the individual.

Q11 **Margaret Mullane:** Given how the public feel about politics at the moment, would you say that still stands? If this is about going for quick wins and winning people over, as the Tony Blair Institute says, should the Government put it in a manifesto if this is so good and beneficial? Equally, it has been suggested that the Home Office is running with this, but it has a lot on and is under a lot of pressure. If you throw this in, it will be another thing to deal with.

Professor Whitley: It is sad and geeky, but this is about who is the correct person to issue attributes. If the state is not the one who determines whether you are a British national, I cannot imagine who would be. It is the state, rather than politics, that issues attributes.

Margaret Mullane: Okay, the Government, then.

Professor Whitley: Yes, the Government are the body who issue these kinds of attributes.

Q12 **Margaret Mullane:** If it is that good, would you agree that the Government should put it in an early offer to the public?

Professor Whitley: Yes. The other point about interaction with the state is that, yes, the Home Office has a gazillion and one other projects—all Government Departments have lots of things that they need to do to improve, digitise and transform their processes—and there is no money to do any of that, and there is a lot of work involved in redesigning systems to operate at a UK scale of 80 million citizens, or whatever it is. I am optimistic, while recognising that there are very practical problems behind the scenes in doing this.

Laura Foster: I think the point to be clear on is that the Government can and should be the source of truth when it comes to citizen data created by the Government, such as your birth certificate. I do not think anyone would be upset that the DVLA gives us our driving licence. Through the gov.uk wallet, the Government are already in the process of digitising driving licences—we will hopefully get a digital driving licence very shortly. That, in itself, is really uncontroversial.

Where the digital verification ecosystem comes in, however, is that you would not then expect the Government to be involved in how I choose to use my physical driving licence. If I want to go to Tesco and buy a bottle of wine, I do not expect the Government to be involved in that transaction. It is the same in the digital case; the Government can give me my digital driving licence, but I do not want them knowing whether I buy my bottle of wine from Tesco. That is where the wider digital identity ecosystem comes in, and that is why we need citizen choice and citizen empowerment. That is why we need to leverage the expertise of the digital ID sector that we already have operating on the trust framework.

Alexander Iosad: There is a strong public appetite to see the state work better, and there is a belief among the public that technology is not being utilised to its full potential to make the state work better. We know that part of that mistrust in the Government comes from the state failing to improve the status quo. Digital ID, in the wider sense that we are discussing it, is a means of improving the interactions between the state and the citizen, so that citizens see the state working for them, not against them.

Q13 **Chris Murray:** Thank you for coming in. In response to Peter's questions, you talked about the benefits in mitigating fraud or immigration offences. Do you think there is any scope, in how this is designed, for it to end up creating opportunities for fraud or immigration offences? Do you think that, by making digital ID our line of defence, there is a possibility for a state actor or data corruption to catastrophically undermine our ability to take on fraud or immigration offences?

Professor Whitley: Anything that becomes a key part of any process will be targeted by fraudsters, organised crime gangs or whatever. The rules that are used to determine whether somebody has the evidence to support their identity claims in the first instance have been evolving over the last 20 years, as we have become aware of different fraud vectors, approaches and attacks.

This will be a target for fraud, and the role of a Government-led process—whether it is private, public or both—is precisely to be aware of where the latest fraud vectors are arising and how best to respond. They might say, "We now need to have three pieces of evidence, when previously we were happy with two." If we suddenly start discovering a whole series of incorrectly issued but genuine British passports, because someone stole them from the passport factory and is giving them to organised crime gang members, you need to double-check not just that it is a genuine passport but, using the passport database, that it was issued to this

person, and that it has not been reported as one of the batch that was lost or stolen. There are lots of things that organisations, both public and private, can do—and are doing—to manage those fraud risks.

Yes, it will absolutely be a target for fraud, because the more important it becomes for our processes, the more valuable it becomes as an opportunity for fraud. To give a simple example from many years ago, when your driving licence used to have a paper counterpart, if you were really concerned about fraud, you would ask to see the paper counterpart as well as the plastic card. There was a market in creating fake plastic cards, but nobody could be bothered to do the paper counterpart. There are things that you can do, because it is essentially a market of transactions going backwards and forwards.

Alexander Iosad: There is an arms race when it comes to fraud. The latest examples might be deepfakes to try to fool systems that use video to identify likeness. I know that our private sector is doing amazingly well in keeping up with that arms race, and there is a really strong argument for the Government to work with them to integrate those technologies into any state-run system that we may end up with.

I would also say that what gives me optimism in this space is that, while anything that becomes central to a process becomes a target, as Professor Whitley says, we also know that the interaction of digital ID in different contexts has reduced fraud significantly. One example of this is in Norway, where the introduction of an ID system reduced payment fraud from 1% to 0.00042% of transactions. That is the type of reduction we can see with digital ID, but it is something that we need to stay on top of, rather than introducing it once and letting it run.

Laura Foster: I do not have an excessive amount to add, apart from to agree that anything that grows in priority is going to be a target for fraud. I also agree that increasingly complex digital fraud vectors require increasingly digital solutions. Again, we are seeing some great solutions from the private sector. I will add that digital verification systems and other types of digital ID systems can be designed in a way that prioritises things such as cyber-security, data minimisation and privacy. One good example of that is something that is called double-blind data sharing. Going back to Tesco and my bottle of wine—

Chair: Other wine retailers are available.

Laura Foster: Sorry, other retailers are available. If I am in Sainsbury's, buying another bottle—

Chair: You're shopping around.

Laura Foster: I am shopping around, getting good deals on my Clubcard, and I again show my driving licence, which shows my name, my date of birth, my address and a lot of other details about me that Tesco does not need to know. If I could show that through a digital credential, all Tesco needs to know is that I am Laura Foster and am over 18. If I can take my

digital credential and use a reliable third-party verification service, it shares the information, which it has checked, that I am over 18 and am Laura Foster, then the supermarket has every right to say, "We trust this data and can let Laura complete this purchase." The supermarket does not need to know anything else about me. That is how digital ID can be trustworthy and implement things such as data minimisation.

Q14 **Chair:** On that test, does the supermarket actually need to know you are Laura Foster? Does it not need to know just that you are over 18?

Laura Foster: They will need to know it is me who is showing the ID in front of them.

Professor Whitley: One option would be that Laura has unlocked her phone, and we assume that—

Chair: Only Laura can unlock her phone. They do not strictly need to know your name, though; they just need to know you are over 18.

Professor Whitley: Absolutely. The simple one would be that I unlock my phone and there is a big, flashing green sign that says, "Over 18", "Under 60", "Over 60", "UK national" or whatever it might be. Somebody has to do the binding, whether it is that they trust that I have unlocked my own phone, or they do a quick visual check to see that it is the same person. In a high-security environment, because I might have stolen Laura's phone and seen her typing in her PIN code, you would really do a careful check, and we would not pass for each other.

Laura Foster: Quickly, and without getting too much into the technical detail on the trust framework—I am very happy to follow up in writing—that verification layer is called an orchestration service provider. Such providers are an important part of the digital ID ecosystem. I am happy to provide more information about that in writing.

Q15 **Chris Murray:** Thank you. That is useful. May I test an argument on you to see what you think? In many ways, the advantages of digital ID that you have set out are basically stuff we can already do, just more efficiently and faster. Is someone a British national? Is someone over 18? Potentially, however, the real thing that would happen here that did not happen before is what you alluded to with your bottle of wine—the interactions could be created and stored. People undertake a lot of activities that are not illegal but that Government may recommend against—if you were buying four bottles of wine every night, maybe the NHS would say, "We should be looking for people who do that, so we can help them." You might be constantly gambling online or accessing pornography, which is clearly something people do not wish to share with others. What would be categorically different in a world with digital ID is that the information is stored, and is therefore accessible.

Professor Whitley: It does not have to be. That is where we come back to the technical design choices. The supermarkets need not have trading standards shouting at them for selling alcohol to under-age people, if they have the assurance that the process at the till is to check that the digital

ID says the customer is over 18 before making the sale. We do not need to have the audit record you are talking about. In practice, we do not have the level of organisational and compliance confidence to say, "No, we trust our processes, and therefore we do not need to have that audit trail of records."

Q16 **Chris Murray:** As a citizen, if all I am asked to do is show a QR code, for example, I have to trust the Government, and I have to trust that it is a bona fide machine and that it is not storing the data somewhere.

Professor Whitley: The Government or the private sector provider.

Chris Murray: Yes, and as it is rolled out, how many times would I show my QR code over the course of a week? I would not be checking what machines I have used—the average person is not going to do that. You are asking the citizen to trust that these machines are not storing data.

Professor Whitley: You are hopefully setting up a framework within which they operate, such that it is clear to everybody that that is not the case. Unfortunately, the announcement of the right-to-work proposals says, "create intelligence data on businesses that are conducting checks". That immediately makes everyone think, "There's probably a record-keeping activity going on." The BritCard proposals, which were one of the influences of this, said, "A digital identity would allow the Home Office to build a canonical record of where and when checks have been successfully completed."

That is one of the elephants in the room. You can design it in a way that says that for things that are low risk, such as when we just want a trusted attribute from a trusted provider, we are happy to say the supermarket has checked that a person is over 18, and we are not going to fine them for trying to sell stuff to under-age kids.

Q17 **Chris Murray:** Are you saying that the capacity to record-keep with digital ID would be a switch that the Government can turn on or off at will?

Professor Whitley: It could be a switch, or there could be a design choice from the very beginning not to build that in. My concern with the right-to-work checks, if they follow these principles, is that by building in the switch for right-to-work checks, everyone is going to ask, "How do we know it is not going to be built in on all the other checks that you suggested, and even if it is switched off, how do we know that this Government or a future Government might not switch it on?"

Laura Foster: You need to have those good governance practices. The eIDAS scheme, which is the European scheme, categorically says that Government cannot collect data on its citizens through any services provided by Government.

I would like to go back to an earlier question, which was: how do you want to take the UK population on this journey with you? It is about putting those safeguards in place so they know that no one is going to be tracking their data. It is about designing those systems so that privacy is there, and sometimes separating out the DVS layers. Critically, it is all about

putting data in the hands of the citizens. That is another advantage of digital ID. If I have a digital wallet, and it can tell me where I have used my digital ID, through being able to live up to the standards of the trust framework, I should be able to enact GDPR and say, "I want all that data gone." That is my right as a citizen, so it is all about establishing what that good governance looks like.

Alexander Iosad: This is exactly why the debate we are having now is so important, because we can have a conversation about the parameters of what would and would not be acceptable on a policy-by-policy basis. There will be trade-offs between privacy, convenience and control in any policy decision, whether it is delivered with digital ID or without.

That is why this debate is about what is possible with this technology. How do we want to draw the trade-offs in any one policy area—whether that is migration or the delivery of public services—and how much control can we give citizens in different circumstances? Again, there are areas of policy in which citizens currently do not exercise any control. That is worth remembering. We can have more control via digital ID than we do today. That is why this debate is so important.

At the same time, once we come to a conclusion on what digital ID should not do, one of the ways to resolve that is by open-sourcing as much of this technology as possible. As we build the platforms, we should be open-sourcing the code so that technical experts—including those who may be sceptical about digital ID—can examine it and show that, yes, there is not a "phone home" element here that says, "Not only did you do a check but it was to buy a bottle of wine, and there are too many of those now." That is something that is possible.

Q18 **Dame Chi Onwurah:** Thank you very much for inviting me, Dame Karen. It is a great pleasure to be here on behalf of the Science, Innovation and Technology Committee. I am afraid that I will try to get into what you have already called the boring technology choices, because they will drive whether this actually works in practice. We have heard a lot about the benefits of digital ID, and I think what you were saying to Margaret and Chris was effectively that the Government were best placed to deliver a digital ID that reflects Government data.

Professor Whitley: It is the best place to issue attributes that Government can issue. I would separate out whether it has to be a Government digital ID.

Q19 **Dame Chi Onwurah:** I recognise that. How significant is the technological effort for the Government to create digital ID? Does making it mandatory increase the significance of that? Are there key technological choices that influence how difficult that is? That is a big question; it would be helpful to have short answers.

Professor Whitley: A big part of how you do ID proofing—confirming who somebody is, so you can then get attributes about them—in the UK uses the standards that I briefly mentioned before: "Good Practice Guide 45", which is a set of rules that determine what evidence will count as

good evidence that you are who you claim to be. A current British passport is really good evidence—not having a British passport means you have to rely on other kinds of documents. Those standards are used for both the Government and the private sector, so they have both had lots of experience of all the processes for checking a passport and different kinds of documents. It also means that you can potentially have two or more digital IDs that satisfy the rules even within one login, because you can have a completely different set of data behind it. It is not difficult, but it is a known problem that has been happening.

The interesting question is to do with the mandatory nature. Everybody talks about the digital divide—people who do not have smartphones or are not confident using them, and so on. The RNIB submission is really telling about the problems of knowing whether you have actually taken a proper selfie if you have sight concerns. That is just one example. You also have people who struggle to have the right mix of documents to satisfy the rules; they may have a smartphone, but they may not have the right kinds of evidence to do it. There was a report for the Government Digital Service a couple of years ago that suggests that almost 6 million people in the UK are ID-challenged. They might get through, but there is a lot of effort and work involved in helping them get that evidence, and if it is mandatory for everybody, a lot of people will struggle to demonstrate that they have an ID that can therefore add the attribute that you have a right to work.

Q20 **Dame Chi Onwurah:** I am a little surprised by your response. You talk about digital ID being a problem that has been solved because we have digital ID attributes, but this is about every Government Department using the same process—using the same data fetch, accessing on the same platform or however it is implemented—and you have not talked at all about the quality of data in Departments. You are just looking at the front end, basically. I am trying to get an overall idea of the challenge.

Professor Whitley: The first challenge, if it is mandatory, is for everybody who needs one, which realistically will be everybody in the country. Even I, who have had my job at LSE for a long time, have had to do other right-to-work checks for other kinds of activities. Calling it voluntary is nonsense; it will be mandatory, because everybody at some point in their life will need another job or to apply for benefits where they have to prove they are able to work. And if you do not have an ID, you cannot get a right to work.

Once you have solved the ID part, you have to match "This is Edgar. Somebody has proved this is definitely Edgar", with the records that you have in our system. This is probably something that will appeal to you: if there are multiple ways that I can prove that I am Edgar, then you cannot have a single unique number that is just my number—the equivalent of the US social security number. That means that every Government Department has to go, "Okay, if it's the same app or the same service that's proved it's Edgar, we can shortcut our processes and go, 'Well, last time, we found his tax records,'" or whatever it is. But if I sign on with a different service, you have to make sure that the back-end services can

cope with, "Oh, there's somebody else called Edgar. Let's see whether we can find that particular record." That is quite a lot of work for every potential relying party that is going to do that.

Given that we have multiple opportunities to create a digital ID, you cannot assume that the back end just has to say, "Once we know who Edgar is, he is person 12345, so that is definitely his record." That is kind of built in, almost as a consequence of the ID proofing standards: because there are multiple ways through the ID proofing standards, there are multiple ways of matching the evidence to the back-end systems. That is going to be a big, big problem.

Q21 **Dame Chi Onwurah:** Laura Foster, do you want to add to that?

Laura Foster: Yes, thank you. There are a few things going on here. I am a bit concerned that we need to separate the use cases of digital ID and the systems of digital ID that the Government have announced from the broader digital transformation of Government. At techUK, we would encourage different Government Departments to find ways to modernise the data stack and open up data sources, especially through smart data schemes in the Data (Use and Access) Act. That complements the digital ID conversation, but digital ID is more of an application of that digital transformation. Please correct me if I am wrong, but if I put that to one side, the question then becomes, how much does a mandatory digital ID scheme cost?

Q22 **Dame Chi Onwurah:** You say that digital ID complements—sits on top of—the digital transformation, so the challenge of digital transformation is part of the challenge of digital ID.

Laura Foster: It can be. Let me take a concrete example of this to try to best explain it. Right now on the gov.uk wallet, it is mandated that by 2027, every single Government Department needs to be able to add any ID—any credential—that it offers physically to the gov.uk wallet digitally. The obvious example of that is the veteran card that we have already seen and the driving licence, but there are so many IDs that you can get from the Government and they all now need to be living on the gov.uk wallet.

Q23 **Dame Chi Onwurah:** That is not going to be easy, so that is a concern. I would like to talk briefly about legacy systems and how they amplify the challenge involved. Do you agree?

Laura Foster: In that particular use case, yes, that definitely would. On the use of digital ID to access other systems, the cost of the digital ID itself is separate from that. There is a whole other infrastructure that the Government are going to have to set up, depending on what level of involvement they decide to take in the digital verification stack. Correct me if I am wrong, but that is kind of what you were referring to, Professor Whitley.

Professor Whitley: Yes.

Laura Foster: I am going to keep coming back to it, but we therefore need to recognise that the UK does already have good governance practices through the trust framework.

Q24 **Dame Chi Onwurah:** Actually, I would not recognise that for two reasons. First, the trust framework is not certified to the European levels that you were talking about, and it is the European levels that address things like deepfakes and so on. The current trust framework certainly cannot be considered, I don't think, to be best practice.

Secondly, as part of the Select Committee's correspondence with the Cabinet Office following the Afghan data breaches and having looked at a review of data resilience that the Government did in 2023, there have been many examples of very, very weak data management practices, to the extent that Government Departments do not even know how many legacy systems they have, so it is impossible to estimate how they can be upgraded to best practice. So no, I would not accept that we have best practice now. How would you respond?

Laura Foster: Apologies. I would definitely say that, yes, in terms of legacy systems, we do not have best practice. TechUK would advocate updating legacy systems. We have a whole team that works on how we can do that, and I would love to follow up in writing with you and share more detailed information on that.

Regarding your point on the trust framework and how it does not adhere to European standards as it stands—and people believe that they are international standards—at this current moment the trust framework does not align with eIDAS or other standards. I believe that there are conversations actively going on within UK Government to understand how the UK's trust framework and the eIDAS scheme can align. That is really important for really simple use cases—for example, in case we want to use our passports in other nations. The trust framework has been created, since 2021, through rigorous consultation with industry and parts of the population as well. The framework has only been legislated on in 2025, so that is quite a long consultation process. We should not scrap something just because it is not perfect. There are redress schemes in place, because things are not perfect. Let us iterate it, build upon it and get the trust framework to a level that it can work within these European schemes as well.

Q25 **Dame Chi Onwurah:** I wonder about the time it will take to do that, but let us move on. Alexander Iosad, do you have anything to add? You talked about open source as a solution. How much of open source is being used right now in Government to support this?

Alexander Iosad: Not as much in this particular area as I think is required to earn the trust of citizens. We would certainly encourage more of that in this space.

If I may add to the discussion on, "Where are we starting and where do we want to get to?" I have two points. One is a mitigating point, hopefully, which is that for the types of system we are discussing here, a lot of the

building blocks are in place already. We have the framework—I agree with Laura that we want to build on and improve it. I also agree that we need to align with the eIDAS standard over time. In my view, any Government-produced ID infrastructure should be eIDAS compliant. We also have ongoing projects to mitigate the impact of legacy systems. We have the blueprint for modern digital government.

Q26 **Dame Chi Onwurah:** Just to say on that, they promised us a plan. The blueprint is a very high level. We were promised a plan, but we do not have a plan yet, do we?

Alexander Iosad: We do not, and I await it as eagerly as I am sure you and members of the Committee do. There is a risk in this debate about digital ID where, if we see it as separate from the broader digital transformation, the digital transformation will head in one direction, the digital ID ambitions will head in another, and they will not connect. In our view, the conversation about digital ID is an opportunity to pay the kind of attention we should have done for a decade or more to digital transformation in Government. The scale of opportunity is immense, we have missed out on a lot of what we should have done, and now is the time to mitigate.

Q27 **Dame Chi Onwurah:** I have two quick follow-ups on that. You are saying that we have in place the building blocks, but my understanding is that for a lot of the legacy systems—the Government's definition of a legacy system is anything that is not on the cloud, but there are probably legacy systems on the cloud as well—we do not know whether they are building blocks that effectively can work.

In terms of them making it mandatory, I think Professor Whitley said that added to the technological challenge, because it meant that so many more people had to be onboarded up front. Are there other ways in which making it mandatory adds to the technological challenge? You talked about somebody called Edgar, in terms of identifying somebody. If they are to be identified, legacy systems in the DWP could have a totally different data format, and we do not even know what that could be yet. In terms of the technological challenge, we need good data management now, and we have not got that. How does making it mandatory amplify the challenge?

Alexander Iosad: I agree with you that we do not have the right level of technical capability within Government right now that we need, and we need to build that up. I agree with you that delivery of the blueprint and the plan behind the blueprint, when it does come, should be a massive priority. Interoperability between Government datasets, which involves, among other things, making sure that the legacy datasets are integrated in the right way, should be a top priority for this Government.

On the mandatory element of this, I think it is worth making a distinction. For the data element, the datasets that hold the attributes are in this case mostly held by the Home Office, whether that is the passport office database, birth records in some cases, the eVisa database or the asylum seekers database. There have been significant challenges with the

delivery, which I believe is partly a result of not enough priority being given to this, including from No. 10 and the Cabinet Office. I hope, possibly against hope, that having a high-profile programme like digital ID would mean that enough attention was paid to these issues. But what we do not know at the moment is whether the mandatory element refers to verifying this information against Government databases—those databases are in place and can be made interoperable in this way, in my view and the view of tech experts I have spoken to, fairly quickly—or whether we are talking about everyone having to have an app and having to carry their phone around, which I hope is not the case.

There is currently not enough clarity about the mandatory element. What do we mean by mandatory? It may be that by mandatory we end up meaning: "We need to be verifying someone's identity and right to work against a Government database, but we can do that in a number of ways, one of which might be a Government app, one of which might be one of the private providers holding a credential, and one of which might be looking at the physical passport and verifying that against the database."

Q28 **Chair:** I am very conscious of time. We have a second panel, and we officially have only four more minutes with you. Would you be happy to stay for a few more minutes and—I am looking at the later panellists—are the later panel happy to start a little later?

Professor Whitley: I have just one other example. Again, I have been around this space for a long time, and another example of the practical problems of systems—these are private sector systems—is all the problems that the pensions dashboard is having. I can prove who I am, but then you have to go to pensions databases that may have very old records, with incorrect data stored on a tape that takes 24 hours to be checked, to then say whether you have a pension with them or not. I have been involved in these conversations since at least before the pandemic, and I think that has all been delayed, delayed and delayed further. It is not just about Government legacy data systems; it is a much broader national problem. I also remember the national data strategy, which I think was before the blueprint for modernising government; so yes, this is a perennial problem, as I think the phrase goes.

Chair: We are going to have to move on, if that is okay. Lewis Atkinson and Margaret Mullane have some questions that go into a bit more detail on the mandatory nature of this.

Q29 **Lewis Atkinson:** Just to be really clear, to what extent are the benefits of digital ID that you have identified contingent on making it mandatory, in your view?

Professor Whitley: I think many of the benefits of digital ID should arise because they are the benefits—because it is an easier way of doing things. You should not need to sell them. My pessimistic view is that as soon as you make it mandatory, you get all sorts of problems of identity exclusion. In my submission, I pointed out the challenges that are already being

voiced around Northern Ireland and the common travel area, and so on, because that will be a big issue.

We saw a bit of coverage about whether you need to do a right-to-work check if you are a 13-year-old getting your first paper round. The next one is: do you need a mandatory proof of right to work before you can claim an income-based benefit? If you do not have a proof of right to work, are you deliberately putting yourself out of the opportunity—

Q30 **Lewis Atkinson:** You are rightly raising some clear challenges with making it mandatory, but can I press you on whether a significant number of the benefits that you have identified, or indeed all of them, would still accrue if there was widespread but not mandatory adoption?

Professor Whitley: For good employers, a digital right-to-work check that is easier than looking at lots of documents is clearly an advantage. For a rogue employer who is employing illegal immigrants, a digital ID is not suddenly going to make them go, "Oh, I'll behave myself and do the appropriate checks and not hire these people." So it will solve some of the problems, but it also forces all the good people to have to do the ID checks, and all the bad people will still be excluded from that conversation.

Laura Foster: I would not disagree. More generally, we should focus more on highlighting the benefits of how a mandatory national ID could be used. You can look at examples that exist within the wider UK. The Government of Jersey have introduced a form of national ID, and they had 55% uptake almost immediately because they found use cases for which it would be very useful. Also, 2.5 million users have been able to access the Improvement Service in Scotland through digital ID. To go back to my first statement, that is because being able to show and prove convenience and time savings to citizens emphasised the use cases for digital ID.

Alexander Iosad: On the migration use case, which we have discussed already, I do not think anyone on the panel believes that it is going to completely solve the problem. There are some advantages, but I would say that they come from the verification against the data, rather than using a particular channel to carry out that verification. There are advantages for some of those good employers as well, because often there is a misunderstanding of what actually counts as a right-to-work check. People think that national insurance numbers are sufficient proof of a right to work, and they break the law when they accept them.

Q31 **Lewis Atkinson:** To check my understanding, you are saying that there could be a mandatory right to check against the central Government record. That might be done very easily via digital ID, for people who choose to use it, but equally it could be done separately, albeit more onerously, via someone saying, "If you don't want a digital ID, bring in two or three different pieces of evidence."

Professor Whitley: As I understand it, the current proposal is that any time you want to take on a job, with a new contract of employment, you will have to have a digital ID, and the only way an employer will be able to

employ you is if they have checked the digital ID. That is the thing that most people are reacting against. There were reports saying, "Don't worry, it's going to be voluntary"—until you have to change a job, which means that everybody is going to have to have it.

Q32 **Lewis Atkinson:** But your view is that you could still do the right-to-work check with a digital ID for some, but via other means for people who did not want to hold a digital ID.

Professor Whitley: Just as we have been doing for the last 10 years. All the ID providers already offer that service.

Laura Foster: You can already use digital ID for right to work through the trust framework.

Alexander Iosad: Where things can be tightened up is in respect of the more—I do not think they are necessarily onerous—analogue checks, which can also result in a verification against the database. The Government will need to figure out what they want to do on that, because they have not, in my view, made it clear enough. When they say, "You have to present digital ID for your right-to-work check," what do they mean by "present digital ID"?

Q33 **Margaret Mullane:** I am the MP for Dagenham and Rainham, which is quite an impoverished area. Since this announcement was made, my inbox has been full of, "No, thank you. You didn't put it in your manifesto." As Professor Whitley just said, it is a sense of unfairness that really upsets people, not the Big Brother aspect of it. As you said, and as I read in the report, rogue employers will carry on regardless, and the good people who follow the rules and do what is right will have a mandatory ID, whether they want it or not. You have all made great points about all the different ways we all provide ID, but the big issue is the mandatory aspect. How do you think the Government should respond to that?

Professor Whitley: It is interesting that I am not sitting between the two positions here. One representative is saying, "It should definitely be the Government, with One Login for Government," which is the current proposal. The private sector is saying it should be done by private companies, or some of these things should be done by private companies. They are both using exactly the same ID proofing standards. So I think I'm going to cop out and say it is a political decision. You could say, "This is something the Government should do, and to heck with the private sector." Or you could say, "We've got a successful private sector. Let's save the Government some money by downplaying the role of One Login, perhaps as an ID provider of last resort for those individuals who want a digital right-to-work check but really aren't targeted by the private sector companies." But there is no logical solution: it is a political choice.

Alexander Iosad: May I gently correct Professor Whitley? I do not believe that this has to be done completely by the Government. I believe that if the benefits that the Government are talking about are to be realised, the most effective route to them is for the data that is held by the Government to be checked as part of the right-to-work check. At the

moment that does not happen, although we still have a mandatory check of the right to work.

That is another part of this debate; we have a mandatory check, it is just that at the moment it is done through one set of documents and there is arguably not enough clarity for employers on what documents count. The Government are talking about changing the list of ways in which you can carry out this already mandatory check. They have not made it clear enough what that list of ways is going to be. I agree with you completely; there is an element of inclusion here that needs to be considered very carefully.

My view is that you can have a Government-run element to this—we can come back to the question of the app, but we probably do not have the time—and do that through existing private sector provider channels as long as the right-to-work credential is issued by the Government.

Laura Foster: I also need to come back and clarify that we do not believe it is an exclusively private sector ecosystem. There is clearly a role for Government in setting what good governance practice and good standards look like, as they already have done, and in legislation. Government may need to be the source of truth when it comes to Government data. We are saying, "If things are working, don't break them." We have the trust framework in place.

I would like to see Government focus on language around empowerment when it comes to digital ID and on the important thing that you mentioned around inclusion. It would be great if we could see Government working with the private sector and other organisations on how we can use innovative things, such as vouching, to make sure that the 6 million people who do not have access to identity can access services.

Q34 **Chris Murray:** I want to follow up on the role of the private sector. You touched on this a little bit, but could the private sector introduce efficiencies that the Government could not, if you wanted to roll this out more broadly? My other question is more on the security side. One of the arguments that proponents of ID cards make is that we all hand over lots of data anyway. Anecdotally and personally, the number of logins that one now uses on a daily basis is huge. Is the fragmentation of that—handing a transport company one set of data, your online banking another set of data and your email login a different set—part of its security, and is that in any way compromised by unifying it all in one Government-backed ID? There are multiple private sector companies. Does unifying that throw the baby out with the bathwater?

Laura Foster: On trying to unify something, it comes down to how it is designed. We would advise against centralised data systems. We would focus on federated architecture and decentralised systems, which means that lots of things are in different places and all have privacy preserving, and that type of thing, in place. Using third-party verified providers that adhere to a good standard can also add a level of privacy preserving.

On your point on how the private sector can bring efficiencies into the system, it 100% can. It is already providing some of the services that have been proposed, efficiently and at no cost to citizens. That may have been a bit of information that was wrongly shared and should be corrected or we have already talked about the use cases in fraud as a really good example, but I will pause there.

Q35 **Chris Murray:** Do you all agree with that? Do you have confidence in the public procurement process in securing those efficiencies?

Professor Whitley: For the record, I would have some concerns about the ability to do effective public procurement, particularly for high-risk, high-security things. It can be done. You need to have the capacity and the expertise in-house to know what you are buying and not just buy from whoever so that you do not get vendor lock-in. It does not necessarily have to be open source, but you need to have independent scrutiny of what is going on, particularly for the security elements. Open source is one way of doing that. For the previous Verify system, the Verify team brought in computer security experts from UCL to review the whole of the technical architecture and point out theoretical, computer science-type risk elements where things could be attacked. They adjusted the processes as a result.

Laura Foster: I would not disagree with that, but I would say that, if you look at international systems, whether that is the Estonia example that has been talked about or more decentralised systems, all digital ID systems that have been created have some form of involvement from the private sector. It is pretty much impossible to do it without that.

Alexander Iosad: One thing that I want to go back to is the point about centralisation. I do not think anyone here is talking about creating one massive central database in Government. We are talking about data that the Government already holds in different places, and there are some challenges around interoperability that we have discussed previously.

What the eIDAS model—where you have the wallet—allows you to do in principle is have more visibility, as Government Departments integrate with the system over time, of what data they actually hold and whether that data is accurate, and, if not, to correct that data. We have recently seen stories of DWP or HMRC deciding that people have left the country when that was not the case. Again, this is something where, with the right technical design, you can build a system that allows you to see that HMRC has decided that you are no longer resident and therefore raise a query with it to say, "No, I am still here."

The wallet model also addresses some of the challenges around the interoperability issue, because it means that you can have Departments issue the credentials—they can be either identity documents or proof of eligibility for a benefit—directly into your wallet, so you can choose when to share it with other Departments. But to me, that is also an argument for there being a Government app that, alongside the private sector,

would mean that these credentials, with citizen control, can be combined in ways that enable more personalised and proactive service delivery.

Q36 **Chair:** We are coming towards the end, but I am interested in the comments about the mandatory nature of the Government's proposals—like Margaret, my postbag has been full of people who are very concerned about them. Obviously, we started the inquiry before the Government announcements were made. From what I understand, none of you is advocating for one entirely mandatory system run by the Government—or am I wrong?

Alexander Iosad: It depends on which layer of that stack we are talking about. The credentials themselves are held by Government, and to achieve some of those benefits you would want there to be consistency that credentials are issued and verified by Government. But the second layer—the interaction between the citizen and the employer—is a much more flexible discussion, and should be.

Laura Foster: Where we disagree is potentially on that verification layer. That comes back to the double-blind data sharing that I was talking about before; there are use cases within that.

Q37 **Chair:** My understanding is that in India private sector expertise was brought into Government and put as a Cabinet-level position so that it had that focus from the top. Clearly that is important.

I want to touch on digital exclusion. My constituency does not have great data coverage and has a population who are not entirely users of smartphones—it is not that kind of constituency—so there is a great deal of concern around this. Do you think that the Government have given any thought to how they deal with digital exclusion? Isn't there a potential Windrush here of people excluded from the whole system?

Professor Whitley: To my thinking, Windrush was more an identity exclusion than a digital exclusion, but they are often very closely related. I am looking at the various committees that I have been on, particularly for the Government Digital Service. I joined the Privacy and Inclusion Advisory Forum in 2023, and the previous Privacy and Consumer Advisory Group had been looking at questions of inclusion and coverage since about 2012, so you would hope that questions of identity exclusion are something that lots of people have been worrying about. In practice, it is one of those extra things where you want to build something and then you worry about the edge cases.

Some research that I did for Women in Identity was about reframing the problem. So you build it as a happy path to get as many people as possible in and covered and do not see it as, "Well, we'll get most of the people in and then just deal with your constituents later on. It's unfortunate, but tough—they are the ones who will have to come in at a second stage."

Q38 **Chair:** Does anyone want to add anything?

Laura Foster: I am a big fan of the Women in Identity work: it really looks at inclusivity by design, which is really important. I have already talked about it. I would actually like to see the Government look at how they can address those who do not have IDs through things such as vouching as part of this.

Alexander Iosad: There are countries, such as Australia, that have done a good job of thinking through these, and we can look to them. I believe the Government are looking at this. One of the first things we saw as the announcement was made, in the explainer that came out on the same day, was that there will be a focus on inclusion and on making sure that people who do not have digital devices are not excluded. Again, for me, it comes back to the distinction between the datasets that are owned and run by the Government, which are not as susceptible to 2G coverage, and the different means of accessing this data in the current context.

Chair: Thank you very much. It feels very fitting that we are doing this session just after we have had a session on Chinese espionage and the ability to get into our phones. Thank you to the panellists. We will move on to the next panel now, and I will bring things to a conclusion while the panellists switch over. Thank you again for your time.

Examination of witnesses

Witnesses: James Baker, Silkie Carlo and Ruth Ehrlich.

Q39 **Chair:** I welcome the second panel of the day. It is probably easiest if you start by introducing yourselves and then we will go into questions.

James Baker: I am James Baker. In the past, I worked for the NO2ID campaign. I now work for an organisation called the Open Rights Group, or ORG for short. We have been going for about 20 years as a not-for-profit, working on digital rights issues and human rights things. Most recently, we undertook research with the University of Leicester and the University of Warwick on a programme called digitising identity, which looked at the Government's eVisa scheme.

Silkie Carlo: I am Silkie Carlo. I am the director of Big Brother Watch. We are a privacy and civil liberties non-profit, non-party campaign group in the UK. I have engaged with the Government over the past 10 years on digital identity matters in various forms, including through being on the privacy and consumer advisory group, and I have engaged with recent data Bills on digital identity verification.

Ruth Ehrlich: I am Ruth Ehrlich. I am the head of policy and campaigns at Liberty, an independent membership organisation. We campaign to defend and extend civil liberties and human rights for everyone in the UK. We played a key role in the NO2ID cards campaign back in the noughties, and we are happy to be back and working on the issue in 2025.

Chair: You were in the room for the previous panel, so you have heard a lot of the questions, but we have some specific questions for you. I will start with Margaret Mullane.

Q40 **Margaret Mullane:** What risk do you think the mandatory element of digital ID presents to somebody's privacy and other rights?

James Baker: We have digital ID already. It is mandatory for migrant workers in the UK under the eVisa scheme, and they already have to present a digital ID via their share codes in order to work. We have real-world examples of where that mandatory scheme has been hurting people. People with the right to work in the UK have lost out on job opportunities because they have not been able to access their share code to prove their right to work. We have had examples of people going into a shop and being asked to show their eVisa share code in order to purchase alcohol, and they have been unable to do it. Where you have mandatory systems introduced like that, it is not hypothetical. We are already seeing real-world examples of exclusion in existence.

Silkie Carlo: The mandatory nature of the proposed digital ID scheme is really the heart of the problem. Digital identities are something that we all use every day in various different ways, but a Government-issued, mandatory digital ID has the potential to create an incredibly intrusive system of surveillance and data collection, and it opens up possibilities for the Government to issue and revoke permissions in certain ways.

Where I would disagree slightly is about the eVisa scheme; it is something that we should certainly talk about, because it has been blighted with very serious issues, which have obstructed people from accessing essential services. But a visa is essentially a permit; we have never had nationals needing to have a permit in this country to go about our everyday lives. The mandatory nature of what has been proposed would introduce that. Suddenly we would be a country that is on licence—where we need a Government permit to do something that otherwise we would have the freedom to do.

Why your inboxes are so full, perhaps, is the mandatory nature of the ID, coupled with a restriction on liberty, which is what the Government have suggested, for something that you would otherwise lawfully be able to do. Unless you have this digital ID card, you will not be able to work. Already other Government Departments are talking about renting, benefits, education, and so on. I think that we would be having a completely different conversation if the Government were talking about a system that they thought was so attractive that, if they made it available, lots of people would want to use it. Instead, it is a mandatory system that is paired with restrictions on people's liberties.

Q41 **Chair:** We have questions on eVisas later, so let's focus on the specifics around the mandatory nature.

Ruth Ehrlich: To echo what has been said, Liberty would not support a mandatory digital ID system, or any mandatory ID system. I think the key thing here is that the specific privacy risks depend solely on the decisions that the Government make now about what this system is going to look like. There is a real opportunity here to create something that centres human rights, that centres privacy, and that centres the way that people

need and want to access their data. But going about it in a way that makes it a mandatory system that is forced upon people to access something very basic such as work will prove a disaster for people on an individual level.

Also, broader privacy risks are raised by creating any kind of database that links to a digital ID system. We know that in the past year alone there has been a 50% increase in cyber-attacks. We have seen the massive impact of cyber-attacks like the Jaguar Land Rover case. This process generally carries significant risks to privacy and cyber-security, which I am sure we will touch on later in this panel.

Q42 **Margaret Mullane:** Do you have any examples of individual rights in other countries that you feel have been affected by digital ID?

James Baker: When you look at examples around the world, a lot of countries that have introduced digital ID have had various issues and problems. Estonia is often held up as this great example, but it had a problem with its chip certification and had to reissue all its chips. This is a small country of a couple of million people. If you had that kind of problem in a country the size of Britain, it would cost hundreds of millions of pounds. When they tried to introduce it in Greece, the Ministry ended up getting fined by its data protection authority. Italy has had a data breach. Venezuela had a data breach when it got attacked; Brazil has; Turkey has. There are a whole host of issues around the world where people have suffered losses resulting from identity cyber-security risks.

In other places, people have faced digital exclusion where they cannot prove their ID. There are plenty of historical examples where ID card systems have been used to marginalise or exclude people—sometimes unintentionally, other times intentionally.

Q43 **Margaret Mullane:** Could you give me an example of it being intentional?

James Baker: We would be going back to historical examples way back in time, but throughout the 20th century there are plenty of examples of ID cards being used to exclude people on the basis of their identity or credentials.

Silkie Carlo: Talking of the Aadhaar scheme in India, something that is often overlooked is that the scheme has even been linked to citizens' deaths through, for example, accessibility problems. It is a massive biometric identity system of over 1 billion people. That has access issues; because it is required for access to welfare, access issues have been documented to have resulted in people actually dying, so they have incredibly serious consequences. Also, that system holds health data and individuals have been refused healthcare because of their HIV/AIDS status, for instance, which is held on this digital identifier.

We see examples of abuses closer to home as well. We have spoken about the cyber-security risks; when individuals are enrolled in mandatory systems, you lose that control over how you manage your data, and you are relying on either the companies or the state. Estonia, which is often

held up as being the gold standard example, has suffered multiple cyber-security incidents where people's photos have been leaked, and so on. On a more individual basis, for example, a police officer in Estonia was fined for checking his fiancée's criminal record. You get access problems as well, where people get unauthorised access to giant databases.

Ruth Ehrlich: To build on that, under the Indian system, you need your Aadhaar ID to pay your tax, to have a bank account and to book certain train tickets. It is part of every single bit of life. Think about people who live in remote areas, people from the poorest communities, people who are illiterate, people who have no digital connection—that is where people become increasingly locked out.

The earlier panel touched on some of those risks in the UK, and there are examples closer to home, as Silkie mentioned. In previous Home Office data projects, things have gone seriously wrong. Look at the data breaches in the Windrush compensation scheme. Dame Chi mentioned the 25,000 Afghan nationals whose data was breached. There are already examples of cases where we are not holding people's data securely. The creation of a system that looks like a centralised system, or a federated system that has broad sharing powers between the systems, poses huge risks.

Q44 **Margaret Mullane:** Finally, how do you see it going forward? Could there be a creep of digital ID that might put people's privacy and human rights at risk? Is that something that worries you?

James Baker: It worries me. We spoke earlier about how digital ID sometimes enables people to do things faster. I use the analogy of lifts: you can get in a lift, and it might get you up to a floor faster, but if something goes wrong with that lift, you still want the stairs as a back-up system to be able to walk up and down. It worries me from a privacy point of view, regarding what a future Government could do with it. There are discussions about how it could be used for this or that, but it is not clear to me that the design scope is clear to everyone yet. Imagine the person you disagree with most in politics—picture them for a moment in your head—and then imagine what they could do with this type of system if you did not have adequate safeguards in place. That is why all of us who care about our rights and the security of the country ought to think about what systems we can put in place to stop that happening.

That is what worries me about introducing this in a country like the UK. We do not have a written constitution that has privacy protections. There is a statute of Parliament—the Human Rights Act—and we have the European convention on human rights, but there is active talk about pulling us out of that convention. I worry that we do not have a resilient-enough rights framework to introduce this type of technology safely in a way that would prevent the risk of a future bad actor misusing these systems, however good the intentions of the current people.

From a resilience point of view, we also need the back-up systems. If your phone battery dies, a server goes down or a foreign Government attacks

your computer infrastructure, it is better for national security that you are not entirely reliant on one centralised ID system and you have multiple systems with which you can prove your ID. At the moment, if I lose one bit of my ID, I can re-establish it through a network. I can go to my bank or, if I lose my driving licence, I have my passport. With a centralised digital ID system, if something goes wrong then you have lost everything and you have no way to prove and re-establish your identity. Those are the risks that we have to avoid.

Silkie Carlo: We are incredibly worried about function creep with this system. Right from the off, the warning signs have been there. This was introduced by the Government as something ostensibly to tackle illegal working, but I do not think that anyone in this room genuinely believes that the mandatory digital ID is about illegal working. That begs the question: what is it really about, and what will the other uses be? This was announced by the Prime Minister on a Friday afternoon and, just hours later, the Government webpage about digital ID was talking about tax, benefits, education, childcare and many other uses for a digital ID.

Function creep is inherent in the system. People will rightly be concerned about that. I have to correct myself: I said that we have never had a mandatory ID, but there was the wartime ID card, of course. Even those ID cards, which were initially issued for rationing, ended up sprawling to 39 Government agencies before they were scrapped by the Churchill Government—so it is inherent in any system.

Those other use cases are concerning. If this starts to pair with a restriction on liberty, what will the other restrictions be? In the minds of many people in this country, the most recent experience of a digital pass was the covid pass. In that case, restrictions were placed on where people could go and what they could do, depending on their vaccination status. There we saw a digital identity system that had very sensitive data and controlled where you could go and what you could do. It was also seen by many to be an attempt to influence decisions. Again, in that case, certain people could not work, such as in health and social care, if they did not have the right vaccination status. Function creep is both inevitable and an overriding concern with this system.

Ruth Ehrlich: I would add that, in terms of function creep, much of this in the hands of the Government now. They can make policy choices that mitigate these risks and create a system that is voluntary and works for the people who choose to use it. One of the core features that this system would need, so that the function creep was not extremely detrimental to people's rights and civil liberties, is something that made sure that the Government could not link previously separate datasets that, if linked, would essentially allow the authorities to build a very detailed, intimate picture of a person based on their healthcare, education and access to welfare and other public services.

We live in an age where we are increasingly seeing predictive algorithms for public decision making. We have lots of examples from the Department for Work and Pensions where that kind of algorithmic decision making has

created serious harm for people accessing welfare. Risk assessments caused 200,000 people to be incorrectly flagged for housing benefit fraud, which led to them having difficulties in paying their rent. We have already seen the risks when you introduce digital systems that are based on algorithms. If you allow all those datasets to be combined, that could be very risky for people's human rights.

Q45 **Dame Chi Onwurah:** The concerns that you have raised on this panel are ones that I know are echoed by my constituents. I wonder what kind of safeguards might help to reassure you, and my constituents, about a digital ID scheme, which has its advantages. Can you think of examples that would help? We have talked about the option to delete all your data that is held by Government, or a system—I think this is the Estonian model—where you are told each time that your data is accessed. That is not the case now; I do not know when Government are looking at my data. Do you think those would help to reassure you and the public about digital ID?

James Baker: There are things you can do to design systems that are more privacy-centric to restore some trust. Part of the problem we have in the UK is that people generally have low trust that, when something goes wrong with their data, it will be well regulated and action will be taken—you see that with things like the Afghan data breaches and the number of Government data breaches in general. There is low trust in the whole information security environment. Part of the problem is that we have an Information Commissioner who is reluctant to take action against Government Departments or organisations, so CEOs do not prioritise it—that is part of it.

The point you made about the logs, or being able to see who has accessed a record and for what purpose, is really important. However, we also have to acknowledge that we live in a legal system where authorities can also check and access people's information essentially in secret through things like the Investigatory Powers Act and RIPA, so people may not even know when their files are being accessed. Things like logs would help.

I think it would help not to have a centralised system but something where Government could issue a credential to a wallet, which you could then see was open source, and you could maybe even build that wallet yourself if it met the framework. It could be issued to something like your Apple or Google account as a credential, or a driving licence, rather than an all-singing, all-dancing ID system.

Part of the problem goes back to the point mentioned about algorithmic data sharing. Quite often, issues of data sharing and Government merging together get conflated with issuing a credential to a digital wallet. When we talk about digital ID, we suddenly end up talking about data sharing, pre-crime algorithms and all that kind of stuff. I think that separating out the debate would help, and separating out the arguments on data sharing from Government being able to issue a digital credential.

Silkie Carlo: It is likely that the way that this announcement has been managed makes it irrecoverable for this Government, and potentially for the next five to 10 years. I am afraid to say that I think the Prime Minister has killed support for digital ID. We can see that in the polls. We also see it in the fact that the e-petition on this issue is the fourth biggest petition in British history and the second biggest petition on a non-Brexit issue. Your constituents are up in arms about it. I think that is because of the way it has been introduced; the fact that no one really believes it is about immigration, and it might be about something else; and how poorly the system has been explained. In that sense, it also makes it difficult to recommend safeguards, because there is not actually a policy here; there has been an announcement.

I have engaged with the Government on digital ID issues, as I say, for a decade. I have spent a lot of time in Government offices with civil servants talking about how a system could be created. We have seen none of that reflected at all in what has happened over recent weeks with this announcement. There has been no detail; there is no substance. If we are talking about what kind of safeguards any theoretical digital ID system could have, we can have a very long conversation about that. Certainly, the starting point would be that it should not be mandatory—that it should be optional, so people can take up a Government-issued digital ID if they feel that it benefits them. It should be something they can exercise total control over; they get to choose who sees their information, and where, when and for what purposes.

Critically, as Ruth was saying, we should not see a merging of Government databases. It is a really big risk with digital ID systems that the taxman can see your GP records and so on. That is also an impetus with these systems, because the argument will be, "Well, why can't the DWP see your health status? Why can't we integrate that?" In many different circumstances, there will be a strong impetus for that data to be shared, but it would have to be strongly legislated around to ensure that it could not happen.

Q46 **Peter Prinsley:** I have a background in the health service as a surgeon. I am interested in how the digital ID might link to the health record—you were talking about that just now. It seems that if we could allow people ownership of their own health record, and that was held digitally, that would give people agency over their own healthcare. That would also be an incentive for people to voluntarily take a digital ID that would be usable across different health agencies. Everybody has an NHS number that was given to them when they were born, and that might be a way into a system such as this.

It seems that encouraging people to engage in a digital ID system could be done by giving people agency over their own healthcare records, such that they were able to go between healthcare providers, hospitals and general practitioners with their own health record. If you knew what was in your health record, you would know a little bit more about your health, and you would probably look after it a bit better. I would like to see the question of how the health record can be incorporated into a digital ID

spoken about a bit more. Do you think that there is any mileage in thinking about it like that?

James Baker: As an organisation, we support people being able to access information about themselves that the Government hold. It is important that citizens are able to see the information that the Government hold about them, and that they understand the basis of how decisions are made about them and what information is used to make those decisions, because that enables people to challenge the decisions when things go wrong.

We looked at health data in Wales for the Welsh Senedd, and we saw examples of problems such as people worrying about going to their doctor because they were worried that the data they might give to their GP or healthcare professional could end up in the hands of Immigration Enforcement. We saw issues with migrant communities that were avoiding accessing healthcare because they were scared it might then be used to check up on their status, or they might end up getting deported as a result of going to the doctor. You see a situation where people lose trust in their healthcare professionals if they think their data is going to be shared with them. MedConfidential have done a huge amount of work around that over the years.

Although there are benefits for an individual being able to access their own data and see how it is accessed and for what purpose, there are massive risks about sharing that data across Government and trying to reimagine that data for different purposes. The public are concerned about that. We see the outcry about some of the big US tech companies like Palantir being involved in the delivery of NHS services, and the worry about how people's data might go into AI systems. That breeds further distrust in Government from the population. I agree that people should be able to access their own data, but it should perhaps not be shared among Government without their consent.

Silkie Carlo: I would agree with that, and also say that the legal position is that people have the right to access their health data. It could be presented in a much easier way, for sure, but I would be very sceptical about that being used in a carrot and stick situation where, if you have easier access to your health data, you enrol in a digital ID that is actually something different from just accessing your health data. You should just be able to access and control your health data regardless of a digital ID.

Ruth Ehrlich: I have two further things to add. First, you then get into the very tricky territory of what you do about those people who are digitally excluded. Are they going to be at a disadvantage if they are not accessing their data in the same way, and you create a two-tier system? There is also the risk of whether you have this kind of system and do not have the firewalls, as James mentioned, between the health record and the Home Office, or indeed the Home Office and pretty much any other service. The Domestic Abuse Commissioner has spoken significantly about how sharing data with immigration officials—with the Home Office—deters survivors of domestic abuse and trafficking from coming forward and

seeking the help that they so desperately need. A "firewall first" approach has to be integral to any system that the Government are looking at.

Q47 **Joani Reid:** I want to focus on linking the digital ID to the right to work. You have been clear on your fundamental concerns and, I suppose, areas of principle that you disagree with. Do you have any specific concerns about linking it to the right to work?

James Baker: It has the potential to marginalise people from being able to participate in the economy. If something goes wrong with their digital ID, they are excluded from being able to earn a living. That, to me, seems a real risk. We know that exclusion is a real problem that happens with digital ID systems around the world. We know that where it has been introduced already, under the eVisa scheme for migrant workers, that is an existing problem. If you roll that out to the whole population then, for anyone who already suffers some form of marginalisation and might struggle to get digital ID, that will further be compounded, because it will be an additional barrier to them accessing work and the economy. That will increase the chances of them falling into poverty or economic disadvantage.

There are particular concerns about gatekeeping the ability of every single British citizen to go out there and earn a living behind some kind of digital system that they have to comply with and get over barriers to access. It is extraordinary when you think about the history of our country that, for years, people have been able to go out there and work, and now we are saying, "No, you lose that right to work as a British citizen," unless they do x, y and z with this digital system. Yes, by all means, employers have to have a system of checks that someone is who they say they are, and those are in place already, but that is an enforcement issue. There is an issue with not enough people going in to check that people are doing the checks, rather than an issue with how checks are done. There are massive concerns for us as an organisation around, essentially, putting the right for someone to go out and work behind a digital ID firewall.

Silkie Carlo: What is being proposed is a multibillion-pound system. It would be right to start with "Why?" rather than "Why not?" I do not think it washes that a British passport is not British enough or good enough documentation to have the right to work, as people currently use it, and that instead you would need this new mandatory digital ID. We have seen, with eVisas, that that has already locked people out of work, because of the accessibility and technical problems with that scheme.

Learning from that, aside from the principles issues, the rights issues and the lack of a basis for why this is necessary for the right to work, we are very concerned about the practical implications. Bear in mind that the Government have been talking about teenagers as well, so it could apply to somebody doing their first paper round, up to a pensioner working in their garden centre. There is a massive scope for who would be forced into a mandatory digital ID scheme.

Ruth Ehrlich: I agree with everything that other panellists have said. The other thing to add is that we know that rogue employers are still going to employ people without checking their right to work. It is a solution that is not going to fix the problem that is being spouted. As Silkie said, that speaks to the more general issue with some of the digital ID proposals that are coming out of the Government. It is being touted as a solution to irregular immigration, illegal working and—at one point—fly-tipping. It also has echoes of the Blair Government in the noughties saying that ID cards were going to fix pretty much any social problem of the day. The Government need to be cautious not to use this as a policy in search of a problem. At the moment, it feels like it is doing that a little bit. It is not going to fix the problems that the Government are saying it will.

Q48 **Joani Reid:** Do you think there is any policy area in which digital ID would be justifiable to help to enforce the law?

James Baker: It is so difficult to answer that question, because what is meant by digital ID is so different. Every country has a different digital ID system, and every country has experienced difficulties in trying to do it. In theory, you could design a system that was fairly privacy friendly, in which Government Departments issued credentials to a variety of public and private sector wallets and there was no tracking, and it was protected by a really good human rights framework, and you had a really well-functioning Information Commissioner so that if things went wrong, they would actually fine someone for their mistakes and hold them to account.

If you had all those things in place, you could imagine a system where it would be more convenient for people to have it as an option on their smartphone and a choice between a physical and digital ID. There are situations in which using digital identity is quicker, and that already exists in society. For example, I have used my bank credentials to do things. I have booked plane tickets online and have used digital credentials to do that kind of stuff. Those kinds of systems are in place already, and some are quicker than going somewhere in person with a physical ID. But you have to have all those other things—your rights framework and your data protection—in place first to make it work.

Silkie Carlo: I have never heard an argument that we could enforce an area of the law so much better if only we had mandatory digital IDs. It is just not something I have come across—unless you go to a very extreme end of the surveillance spectrum. That is one of the things I am really worried about here, in so much as what we know about the proposed digital ID system is that it will basically be a massive facial recognition system, because it would be linked to facial biometrics. That is one of the only substantive things we have been told about the Government proposal. That means you would have around 50 million British adults with their sensitive personal biometric data in a system and, quite unusually, millions of foreign nationals as well. It is not a British-only system, because it relates to everyone working here.

Given that this is being introduced when the Government are also backing a significant expansion of facial recognition surveillance in this country,

and we have found that the Government are now using the passport database for facial recognition searches, without having discussed it with Parliament, from a law enforcement perspective, I would be very worried about how this gargantuan new biometric system could also be used for that extension of surveillance.

Ruth Ehrlich: There is not a model of digital ID that a civil liberties organisation would support that would specifically meet that policy objective. When we look at a good system, we look at something that is voluntary and has firewalls.

Q49 **Joani Reid:** That is very clear; thank you. You have mentioned eVisas quite a few times, and you have talked about people being locked out of work because the system had broken down or whatever. Are there other impacts on individuals using eVisas, beyond the examples you have already given?

James Baker: There have been examples involving issues of domestic abuse, where someone in a household is denied an eVisa, because essentially it is on a phone and an abusive partner controls access to that device. There is potential there when it comes to digital systems, because you can control people through their access to digital devices. There are issues with that.

We have had issues of function creep, with private sector organisations demanding that people produce their eVisas in situations where they are not required, such as in the process of applying for a job rather than when they have got the job. I gave the example of someone being prevented from buying alcohol because they could not get internet access and show their eVisa share code. That is an example of a private sector organisation taking it upon themselves to enact a Government-mandated digital ID to deliver their service. They are the examples I'd give of where it has hurt people in the real world.

Silkie Carlo: A group called the3million has published a brilliant report called "Digital Status Crisis", which has a lot of important information and case studies in this area. It seems to me that, of the areas from that report that are most applicable to digital ID, one is the data-matching issues. People are logging in to their eVisa and finding somebody else's migration status and somebody else's photograph. There are very basic data issues.

The second tier of issues is around access failures, whether on the user side—obvious things like if your phone runs out of battery or you do not have good internet access—or on the system side. If there is a system issue, people are finding it very, very hard to get in touch with the Home Office and try to do something about it. There are case studies in the report of people having been locked out of work, travel and education, for example.

Ruth Ehrlich: In addition to that, people have been wrongly told they have refugee status, been unable to travel back to the UK from holiday,

been charged for NHS treatment when they should not be—the kind of untold human misery that the system not working has caused. That highlights the risk of creating a digital product like this.

I am sure that many of you have, through casework or through family or friends, supported people to apply for an eVisa. It is a nightmare. It is so difficult to do. Even for the most digitally literate, and for people who work in the sector, it is unbelievably hard. It is a perfect illustration of how a poorly designed mandatory system leaves people at an enormous disadvantage.

Q50 **Joani Reid:** Do you think the problems are intrinsic, or can a far better system be designed that does not have those problems?

Ruth Ehrlich: The starting place is wrong if you do not approach it from a place of, "How do we make this a system that is going to improve access to services, work for people and centre human rights?" If you start from that place, you might be able to build something much better, but this has been built from the wrong starting point.

James Baker: The larger the systems get, that creates other problems. Estonia is a couple of million people, and the eVisa scheme is roughly 4 million people; what the Government are talking about is a system that would cover 50 million, 60 million or 70 million people. Some of the problems—the issues of duplicate records, matching people, biometric mismatches, and all that stuff—expand the larger the data set is. You see that in the India scheme: it is not necessarily a unique ID, because they can match someone in India to about 1,200 other people through the biometric mismatching, because these systems are not perfect in matching someone's biometric credentials. If you use something like facial biometrics, as proposed here, there will be, given the scale of the population, a lot of mismatches and problems when you scale it up.

Chair: Lewis Atkinson and Chi want to come in, and I think Peter wants to come in as well. I am conscious that we do not have that long.

Q51 **Lewis Atkinson:** Can I be clear on the mandatory work checks? I hear really clearly that you are against mandatory digital ID for those checks—that's taken as read. You will have heard the previous panel talk about a potential interpretation, or policy direction of Government, that mandatory work checks would have to be checked with Government, which could be done via a digital ID for those who choose to take one up, but could also be done via other means, such as a passport, but checked back with the Government. How would you react to that? How far do you think that would mitigate some of your privacy and other concerns?

James Baker: It would be great to allow people a multitude of ways to prove their ability to work. It would be fantastic and really sensible not to make them rely on an eVisa if they have a passport, driving licence or anything else. I would raise a little bit of concern as to what then happens with the data that goes back to Government, and what it is used for. Is that going into an AI algorithmic system to try to automatically detect discrepancies with their bank accounts to work out who is or is not

working illegally? If that is the intention, you will start wrongly flagging and wrongly prosecuting a load of people, as we saw recently with the HMRC scandal when people leaving the country got flagged as not being entitled to their benefits when they were. What will that data be used for and for what purpose? That is the real question.

Silkie Carlo: I agree with that. It would seem strange that, as it currently stands, you can use a British passport for a right-to-work check, to travel, to apply for a bank account or financial services, and so on, but it wouldn't be good enough for somebody to do a paper round and you would need this extra layer of Government checks. Likewise, that would be likely to sprawl, because if you need a Government check for that, why not for things such as healthcare and renting?

I completely agree that having a multitude of ways to identify yourself is a very good thing. If the Government want to offer people some form of digital identity in a very different way, some will find that helpful, but having a Government link to that data raises many of the same concerns as mandatory digital ID.

Q52 **Dame Chi Onwurah:** Just to follow up on that, I have set out my concerns about digital IDs, but you seem to be saying that any form of digital ID is concerning—you seem to be opposed to any form of digital ID. It has to be said that paper-based systems, which is what the Windrush system was originally, involve big concerns and have caused many problems for constituents. Ruth, you said you would start from a different place by designing it on the basis of supporting human rights. Can you just confirm that you are not opposed in principle to any form of digital ID, and say a little bit about what would make it work for your organisation?

Ruth Ehrlich: Liberty is not opposed to all forms of digital ID. We think there is, in fact, a way of creating a system whereby people can share less data about themselves in a more helpful way. You talked about that a bit with the last panel. When you go to rent a property, you give your letting agent a huge amount of data that they do not need. There is a way to create a system that is much more narrow, but that ID system would need to follow the principle that it is voluntary. This is not to hammer home the point, but it should be opt-in. It should be privacy-first, with firewalls to stop data sharing between Government Departments that do not need to be sharing data. It should be GDPR-compliant and so have the privacy-by-design principles. That is the baseline of what we would need to see.

Silkie Carlo: I started by saying that digital identity is something that many of us use every single day, so there is not an in-principle aversion to digital identity per se at all, but when you have a Government scheme, especially if it is mandatory, it is our job as human rights defenders to identify where those risks are.

Q53 **Dame Chi Onwurah:** But you are not opposed to a Government digital ID scheme in principle?

Silkie Carlo: In principle, it is possible for the Government to offer people a digital identity that they could choose to use, but that is a very broad

conversation. It is a million miles away from what has been proposed by this Government.

James Baker: We have the same kind of position. We are in danger, perhaps, of losing some of the institutional memory around how to do this right. The Privacy Advisory Group came up with the principles around how to do identity assurance. They were published and they are still on DSIT's webpage. There is a whole list of those there already, so work has been done around how you could do this in a better way that respected people's rights.

If it were voluntary—if it were something that I could choose to have or not—and if I were able to see the code behind the wallet, choose what wallet I wanted to issue to, and it wasn't about data sharing and my data then being used for other purposes, I would be far more willing to accept it, but that is not the scheme that appears to be on the table at the moment. Possibly things can change.

Q54 **Peter Prinsley:** You have reflected what I was going to ask. It seems to me that you are not opposed to a voluntary digital ID system for this country that people can opt into, provided it has certain safeguards about how the data was distributed and used. If we were to create a voluntary opt-in digital ID service for the British people, what proportion do you think would be interested in adopting it? Do you think it would be around 5%, or do you think it would grow?

James Baker: It would depend, in some ways. The danger is that you would have function creep—take the example I gave earlier of someone being required to use their eVisa to buy alcohol. You might then see, when buying something from Ticketmaster or from other organisations, that they say, "Well, actually, we only accept that digital ID now."

You would have to legislate in a way that did not discriminate against people who choose not to have a digital ID, and you would also have to ensure that a future Government could not come along and change the parameters of that digital ID to make it quite an abhorrent thing that would not be the type of system most of us would want to see in this country.

There are a lot of risks. You have to think about the rights framework and the data protection safeguards that need to exist within society to make this safe. If you got those things right, you would see higher adoption. If you had a society where data protection breaches go unpunished and human rights are not respected, you would see a lot more scepticism and resistance from people to taking up such a system.

Q55 **Peter Prinsley:** On the first panel, we heard about many of the advantages of digital ID; on this one, we have been well apprised of the problems—you have been very successful with that venture. If people could be made to see the advantages for themselves, as individuals, my guess is that, with the appropriate safeguards, adoption would increase. Do you agree with that?

James Baker: On the language "made to see", I think people can see for themselves whether they trust something or not. Unfortunately, from this scheme, as you can see from the petition and the way people have reacted, they do not trust it. Perhaps in the future there will be another scheme that has people's trust, but they would need to trust the entire rights framework and the data protection framework behind it. Then you might see people adopt it and enjoy the benefits.

Silkie Carlo: Currently, none of our lives are adversely affected by not having a Government-issued digital ID, and many of us have Government-issued identity documents that we use in different scenarios—for instance, passports, birth certificates and so on. It does seem like a policy in search of a problem to solve.

What I would then worry about is that when you talk about making people see the benefits—we spoke about health data being used—what has happened with voluntary schemes, such as the Aadhaar scheme in India, is that although it is ostensibly voluntary, in practice it is not. Everyone has to have it to access basic services, and you can end up in a situation where something introduced as voluntary is used to gatekeep many different services.

If you think about the situation we would have been in if we had had a digital ID system when the pandemic started, there are ways in which that ID would have been used in those circumstances: we had track and trace, vaccine passports, and so on. The risk is that, in response to any future moral panic, there will be a temptation to say, "Why don't we add this to the digital ID?", or, "Why don't we use it in this way?" We have seen that in some of the examples around the world.

Ruth Ehrlich: Seeing the public's response to the Government's announcement shows that we are a nation that is still very sceptical of any kind of mandatory ID, which is obviously lovely for organisations such as Big Brother Watch and Liberty to see. However, I would say that the Government could look to the EU approach to digital ID, which prioritises privacy and security, to look for ways to ensure a system is built where the user has control over their data, it is genuinely voluntary, and safeguards are in place to protect against discrimination for people who choose not to opt in. There are models that are better than others, which are always worth looking at.

Chair: Finally, on digital exclusion, Lewis Atkinson.

Q56 **Lewis Atkinson:** Can you outline how you think the Government should account for digital exclusion when developing their plans for digital ID—whether that be mandatory or not?

James Baker: One simple thing: do not make it mandatory. That would immediately mean something for all those people who might be excluded by your design choices on the technology, the operating system it can work on, or how the software works—even getting a photograph is a challenge for some people. With eVisas, we heard examples of people with

severe learning disabilities or autism—it is hard just to get them to sit still to take the photograph needed in the right style and so on. Not making it mandatory massively makes it easier for the Government to tackle a load of those digital exclusion issues.

Silkie Carlo: I agree. Also, the facial recognition aspect could introduce some exclusion factors, given the issues with misidentifications and facial recognition, particularly on race and gender, as well as certain disabilities.

Inclusion in a system does not always need to mean that people are forced into a digital or technological system, for example. There would have to be an offline alternative for the many people who do not have good connectivity or good digital skills, and to acknowledge that many people do not want to be forced into a system like that. Some people do not want to have smartphones—the whole conversation about smartphones is changing—but the idea is that everyone would have a smartphone with a very essential piece of data on it, so that might not stand the test of time.

Ruth Ehrlich: The question of digital exclusion goes beyond the remit of Liberty in many ways, because we are talking about poverty more generally and about lack of access to a good connection. Touching on what Silkie said, even with a mandatory system with a fall-back of having a physical ID card, the previous Government's own research on voter ID in the run-up to the previous election showed that there were already massive barriers to people who are excluded through, yes, having disabilities, being unemployed, not having qualifications or being first-time voters. That cohort of people are much less likely to have any form of ID, so it is not as simple as creating a system just with an option to have a paper ID.

Q57 **Chair:** Thank you. Did anything come out of the previous panel that you would like to respond to?

James Baker: Just one point. We talked about the personal privacy risk, but there is a cyber-security risk for the whole nation. The more you make everyone reliant on a particular way of doing digital ID, the more you increase the attack vectors for a foreign adversary to take out that system and to target it in an act of cyber-warfare. The system being mandatory or non-mandatory is not just about digital exclusion or individual rights; it is also about building systems that are resilient to foreign attack and that can carry on working in a disaster situation. To go back to my analogy, digital ID might be lifts, but we still want stairs in the case of a fire or something—we need alternatives.

Chair: I thank the second panel very much for their contributions. I found it incredibly interesting and informative. As the opening piece of oral evidence for this inquiry, this has been a very good way of starting us off on our next steps. Thank you.