# PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

## Public Bill Committee

# DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

*Second Sitting*

*Wednesday 10 May 2023*

*(Afternoon)*

CONTENTS

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

**not later than**

**Sunday 14 May 2023**

**The Committee consisted of the following Members:**

*Chairs:* † Mr Philip Hollobone, Ian Paisley

Amesbury, Mike *(Weaver Vale)* (Lab)
† Bristow, Paul *(Peterborough)* (Con)
† Clarke, Theo *(Stafford)* (Con)
† Collins, Damian *(Folkestone and Hythe)* (Con)
† Double, Steve *(Lord Commissioner of His Majesty's Treasury)*
† Eastwood, Mark *(Dewsbury)* (Con)
Henry, Darren *(Broxtowe)* (Con)
Hunt, Jane *(Loughborough)* (Con)
† Huq, Dr Rupa *(Ealing Central and Acton)* (Lab)
† Long Bailey, Rebecca *(Salford and Eccles)* (Lab)
† Monaghan, Carol *(Glasgow North West)* (SNP)
† Onwurah, Chi *(Newcastle upon Tyne Central)* (Lab)
† Peacock, Stephanie *(Barnsley East)* (Lab)
† Richards, Nicola *(West Bromwich East)* (Con)
Simmonds, David *(Ruislip, Northwood and Pinner)* (Con)
† Wakeford, Christian *(Bury South)* (Lab)
† Whittingdale, Sir John *(Minister for Data and Digital Infrastructure)*

Huw Yardley, Bradley Albrow, *Committee Clerks*

**† attended the Committee**

**Witnesses**

Tom Schumacher, Chief Privacy Officer, Medtronic

Jonathan Sellors MBE, Legal Counsel and Company Secretary, UK Biobank

Harry Weber-Brown, Chief Engagement Officer, ZILO

Phillip Mind, Director, Digital Technology and Innovation, UK Finance

Keith Rosser, Chair, Better Hiring Institute

Helen Hitching, Deputy Director and Chief Data Officer, National Crime Agency

Aimee Reed, Director of Data, Metropolitan Police

Andrew Pakes, Director of Communications and Research, Prospect

Mary Towers, Policy Officer, TUC

Alexandra Sinclair, Research Fellow, Public Law Project

Ms Laura Irvine, convener of the Privacy Law sub-committee, Law Society of Scotland

Jacob Smith, UK Accountability Team Leader, Rights and Security International

Alex Lawrence-Archer, Solicitor for AWO (a data rights agency)

# Public Bill Committee

*Wednesday 10 May 2023*

*(Afternoon)*

[Mr Philip Hollobone *in the Chair*]

## Data Protection and Digital Information (No. 2) Bill

### Examination of Witnesses

*Tom Schumacher and Jonathan Sellors gave evidence.*

2 pm

**The Chair:** Welcome back. We are now on to our fifth witness panel and we will hear from Tom Schumacher, chief privacy officer at Medtronic, who has kindly joined via Zoom, and Jonathan Sellors, legal counsel and company secretary at UK Biobank, who is in the room. We have until 2.25 pm for this panel. Could the witnesses please introduce themselves for the record?

***Jonathan Sellors:*** Good afternoon. I am Jonathan Sellors, general counsel of UK Biobank. To those who may not know, we are the largest globally accessible clinical research resource in the world. We comprise 500,000 UK-based participants, and we make de-identified data available to researchers to conduct clinical research in the public interest.

***Tom Schumacher:*** Thank you so much for inviting me. I am Tom Schumacher, and I work for Medtronic as the chief data and privacy counsel. Medtronic is the world's largest medical device maker, with 90,000 employees around the world and three manufacturing sites in the UK. We are headquartered in Ireland.

**The Chair:** Thank you both for joining us. Stephanie Peacock.

**Q82 Stephanie Peacock** (Barnsley East) (Lab): Welcome to you both. My first question is to both witnesses. How easy is it currently for service users and care teams to access and share all of their relevant health and care data?

***Jonathan Sellors:*** I am not sure I am the expert on this particular topic, because my experience is more research-based than in IT systems embedded in clinical care.

***Tom Schumacher:*** I am also not as intimately familiar with that issue, but I would say that interoperability is absolutely critical. One of the challenges we experience with our technologies—I assume this is also the case for your health providers—is the ability to have high-quality data that means the same thing in different systems. That is a challenge that will be improved, but it is really a data challenge more than a privacy challenge. That is how I see it.

**Q83 Stephanie Peacock:** Will the new definition in the Bill of what constitutes scientific research help people in your field to conduct more or better research? If so, what impact would this research have on citizens and healthcare?

***Jonathan Sellors:*** I think it is a thoroughly useful clarification of what constitutes research. It is essentially welcome, because it was not entirely clear under the provisions of the General Data Protection Regulation what the parameters of research were, so this is a helpful clarification.

***Tom Schumacher:*** I completely concur: it is very useful. I would say that a couple of things really stand out. One is that it makes it clear that private industry and other companies can participate in research. That is really important, particularly for a company like Medtronic because, in order to bring our products through to help patients, we need to conduct research, have real-world data and be able to present that to regulators for approval. It will be extremely helpful to have that broader definition.

The other component of the definition that is quite helpful is that it makes it explicit that technology development and other applied research constitutes research. I know there is a lot of administrative churn trying to figure out what constitutes research and what does not, and I think this is a really helpful piece of clarification.

**Q84 The Minister for Data and Digital Infrastructure (Sir John Whittingdale):** Perhaps I could ask you both to elaborate on how the existing definition and the current lack of clarity have impeded you in carrying out the research you would like to do and how this will change as a result of the Bill.

***Tom Schumacher:*** Maybe I can give an example. One of the businesses we purchased is a business based in the UK called Digital Surgery. It uses inter-body videos to try to improve the surgery process and create technologies to aid surgeons in prevention and care. One of the challenges has been, to what extent is the use of surgery videos to create artificial intelligence and a better outcome for patient research? Ultimately, it was often the case that a particular site or hospital would agree, but it created a lot of churn, activity and work back and forth to explain exactly what was to be done. I think this will make it much clearer and easier for a hospital to say, "We understand this is an appropriate research use" and to be in a position to share that data according to all the protections that the GDPR provides around securing and de-identifying the data and so on.

***Jonathan Sellors:*** I think our access test, which we apply to all our 35,000 users, is to ensure they are bona fide researchers conducting health-related research in the public interest. We quite often get asked whether the research they are planning to conduct is legitimate research. For example, a lot of genetic research, rather than being based on a particular hypothesis, is hypothesis-generating—they look at the data first and then decide what they want to investigate. This definition definitely helps clear up quite a few—not major, but minor—confusions that we have. They arise quite regularly, so I think it is a thoroughly helpful development to be able to point to something with this sort of clarity.

**Q85 Sir John Whittingdale:** Can you say a little about the extent to which you have been a contributor to the design of the new provisions in the Bill and whether you are happy with the outcome of that?

***Jonathan Sellors:*** The short answer would be yes. I was contacted by NHS England about the wording of some of the consent aspects, some of the research aspects and particularly some of the pseudonymisation

aspects, because that is an important wall. Most research conducted is essentially on pseudonymised rather than identifiable data. The way it has been worded and clarified, because it makes an incremental improvement on what is already there in the GDPR, is very useful. I think it is a good job.

***Tom Schumacher:*** Yes, I would say the same. NHS Transformation and the Department for Culture, Media and Sport, particularly Owen Rowland and Elisabeth Stafford, have been very willing to hear points of view from industry and very proactive in reaching out for our feedback. I feel like the result reflects that good co-ordination.

**Q86 Damian Collins** (Folkestone and Hythe) (Con): Do you think the definition of what public health means in the context of the Bill is clear?

***Jonathan Sellors:*** Yes, I think it is reasonably clear.

**Damian Collins:** What do you mean by that?

***Jonathan Sellors:*** Like any lawyer, if I were asked to draft something, I would probably always look at it and say I could possibly improve it. However, I would actually look at this and say it is probably good enough.

**Q87 Damian Collins:** What do you think it means? What is the scope of it?

***Jonathan Sellors:*** If I may, can I come back to you on that with a written response, when I have given it slightly further consideration? Would that be okay?

**Q88 Damian Collins:** Yes. What I would be interested in is that there could be medical research linked to physical ailments. It could also include mental health, which could, in this context, open up quite a wide range of different fields of research for commercial application as well—understanding people's stimulus response to fear, anxiety and so on, some of which could have medical application and some of which could be purely commercial.

***Jonathan Sellors:*** I think that, with health-related research that is in the public interest, it is relatively straightforward to spot what it is. Most research is going to have some commercial application because most of the pharma, molecules and medical devices are going to be commercially devised and developed. I do not think that the fact that something has a commercial interest should count it out in any way; it is just about looking at what the predominant interest is.

**Q89 Damian Collins:** I think that is right. I would welcome it if you were able to write to the Committee with some further thoughts on that. My point, I suppose, is that we have a pretty good idea of what we think public health research could be in this context, whether it is for commercial or non-commercial reasons. However, we want to be certain about whether that opens up other channels of research that others may regard as being not about solving public health problems, but just about the commercial exploitation of data.

***Jonathan Sellors:*** Right, thank you. I understand.

***Tom Schumacher:*** I concur with what the previous speaker said. In the medical device industry, we really focus on what is considered more traditional research, which fits well within the refined research definition that the Bill contains.

**Q90 Damian Collins:** I have a final question. We have this legislation, and then different tech companies and operating systems have separate guidelines that they work to as well. One of the issues the Government faced with, for instance, the covid vaccine app, was that it had to comply with the operating rules for Google and iOS, regardless of what the Government wanted it to do. Thinking of the work that your organisation has been involved in, are there still significant restrictions that go beyond the legal thresholds because different operating systems set different requirements?

***Jonathan Sellors:*** I do not think I am really the best qualified person to talk about the different Android and Apple operating systems, although we did a lot of covid-related work during the pandemic, which we were not restricted from doing.

***Tom Schumacher:*** I would say that this comes up quite a lot for Medtronic in the broader medtech industry. I would say a couple of things. First, this is an implementation issue more than a Bill issue, but the harmonisation of technical standards is absolutely critical. One of the challenges that we, and I am sure NHS trusts, experience is variability in technical and IT security standards. One of the real opportunities to streamline is to harmonise those standards, so that each trust does not have to decide for itself which international standard to use and which local standard to use.

I would also say that there is a lot of work globally to try to reach international standards, and the more that there can be consistency in standards, the less bureaucracy there will be and the better the protection will be, particularly for medical device companies. We need to build those standards into our product portfolio and design requirements and have them approved by notified bodies, so it is important that the UK does not create a new and different set of standards but participates in setting great international standards.

**Q91 Rebecca Long Bailey** (Salford and Eccles) (Lab): In relation to medical research, concerns have been raised that the Bill might risk a divergence from current EU adequacy and that that might have quite a significant detrimental impact on collaboration, which often happens across the EU on medical research. Are you concerned about that, and what should the Government do to mitigate it?

***Jonathan Sellors:*** I think that it is absolutely right to be concerned about whether there will be issues with adequacy, but my evaluation, and all the analysis that I have read from third parties, particularly some third-party lawyers, suggests that the Bill does not or should not have any impact on the adequacy decision at all—broadly because it takes the sensible approach of taking the existing GDPR and then making incremental explanations of what certain things actually mean. There are various provisions of GDPR—for example, on genetic data and pseudonymisation—that are there in just one sentence. It is quite a complicated topic, so having clarification is thoroughly useful, and I do not think that that should have any impact on the adequacy side of it. I think it is a very important point.

***Tom Schumacher:*** I agree that it is a critical point. I also feel as though the real value here is in clarifying what is already permitted in the European GDPR but doing it in a way that preserves adequacy, streamlines and makes it easier for all stakeholders to reach a quick

and accurate decision. I think that adequacy will be critical. I just do not think that the language of the text today impacts the ability of it to be adequate.

**Q92 Chi Onwurah** (Newcastle upon Tyne Central) (Lab): I know that you are very supportive of the Bill, but I wonder whether you see risks to patients and service users from facilitating a greater sharing of health and care data. Could you each answer that question?

***Jonathan Sellors:*** I think that data sharing, of one sort or another, absolutely underpins medical research. You need to be able to do it internationally as well; it is not purely a UK-centric activity. The key is in making sure that the data that you are using is properly de-identified, so that research can be conducted on patients, participants and resources in a way that does not then link back to their health data and other data.

**Q93 Chi Onwurah:** So it has to be de-identified. We will return to that. But you do not see any other risks?

***Jonathan Sellors:*** Let me put it this way: poor-quality research, undertaken in an unfortunate way, is always going to be a problem, but good-quality research, which has proper ethical approval and which is done on data that is suitably managed and collated, is an essential thing to be able to do.

**Q94 Chi Onwurah:** I agree with you. Sorry, I did not quite hear what you said—approval by whom?

***Jonathan Sellors:*** Approval by the relevant ethics committee.

**Q95 Chi Onwurah:** Right. Is it a requirement of the Bill that the research should have the approval of the relevant ethics committee?

***Jonathan Sellors:*** I do not think that it is a requirement of this Bill, but it is a requirement of pretty much most research that takes place in the UK.

**Q96 Chi Onwurah:** But not all research, surely, because the definition of research is something that can

"reasonably be described as scientific"

research. You would see concerns, then, if data was to be shared for research that was carried out outside of ethics committee approvals. I do not want to put words into your mouth, but I am just trying to understand.

***Jonathan Sellors:*** Sure. I think it depends on the nature of the data that you are trying to evaluate. In other words, if you are looking at aggregated or summary datasets, I do not think there is any particular issue, but when you are looking at individual-level data, that has to be suitably de-identified in order for research to be safely conducted.

**Q97 Chi Onwurah:** On the point of de-identifying or pseudonymisation, do you recognise that there have been examples of pseudonymised data that has been re-identified, and that, particularly given the rise of huge datasets, artificial intelligence and so on, there is a risk of un-de-identifying pseudonymised data?

***Jonathan Sellors:*** There is always a risk, but I think the way it is expressed in the Bill is actually quite measured. In other words, it takes a reasonable approach to what steps can constitute re-identification. There are a certain police-related examples whereby samples are found on crime scenes. The individuals can be identified, certainly, if you are on the police database, but if they are not on a reference database, it is extremely difficult to re-identify them, other than with millions of pounds-worth of police work. For all practical purposes, it is actually de-identified. Saying something is completely de-identified is quite difficult.

**Q98 Chi Onwurah:** Yes, I certainly agree with that—it is almost impossible—but I do think it is possible to re-identify data without spending millions of pounds, especially when it is correlated with other large datasets. Would you recognise that?

***Jonathan Sellors:*** I definitely recognise that. That is one of our principal bits of concern, but usually the identifiers are the relatively simple ones. In other words, you can re-identify me quite easily by my seven-digit postcode and my age and my gender. Obviously, when we release data, we make sure not to do that. Releasing quite a big bit of my genetic sequence does not make me re-identifiable.

**Chi Onwurah:** Currently.

***Jonathan Sellors:*** Currently—I accept that.

***Tom Schumacher:*** I would say a couple of things. It is important to know that the Bill preserves the full array of safeguards in the GDPR around data minimisation, access controls and making sure that you have de-identified the data as much as possible for the purpose you are going to use it for. The opportunity that our company is quite concerned about is that, without some elements of real-world data, we are not going to be able to eliminate the bias that we see in the system. We are not going to be able to personalise medicine, and we are not going to be able to get our products approved, because our regulating bodies are now looking at and mandating that the technology we use is tested in different attributes that are relevant for that technology.

As an example, there are very few data pieces that we need for our digital surgery business, but we might need gender, weight and age. The Bill will allow customisation to say, "Okay, what are you going to do to make sure that only two or three data scientists see that data? How are you going to house it in a secure, separate environment? How are you going to make sure that you have security controls around that?" I think the Bill allows that flexibility to try to create personalised medicine, but I do not believe that the Bill opens up a new area of risk for re-identification provided that the GDPR safeguards remain.

**Q99 Chi Onwurah:** Let me ask a follow-up question. I recognise that your intent in research is ethical—there are ethics committees involved. Given the definition of scientific research to be anything that can be reasonably described as scientific, what is to stop data being shared for the purposes of, for example, justifying anti-covid vaccination conspiracy theories? Do you recognise that there are purposes that could be described as research but which many people would not want their data to be used for?

***Tom Schumacher:*** In isolation, that would be a risk, but in the full context of the interrelationship between the data owner and controller and the manufacturer, there would be a process by which you would define the

legitimate use you are going to use that data for, and that would be something that you would document and would go on your system. I do not believe that using data for political purposes would constitute research in the way that you would think about it in this Bill. Certainly the UK ICO is well regarded for providing useful interpretation guidance. I think that that office would be able to issue appropriate guardrails to limit those sorts of abuses.

***Jonathan Sellors:*** If you look at a scientific hypothesis, it might not be a scientific hypothesis that you like, but it is much better to have it out there in the public domain, where the data that underpins the research can be evaluated by everybody else to show that it is not sound and is not being conducted appropriately.

**Q100 Chi Onwurah:** Yes, but people might not want their data to be used for that. They would have no control over it in this case.

***Jonathan Sellors:*** There has to be some element of scientific flexibility, but scientists themselves have to be able to make a decision about what they wish to investigate. The main thing to ensure is that it is transparent—in other words, somebody else can see what they have done and the way in which they have done it, so that if it does come up with a conclusion that is fundamentally flawed, that can be properly challenged.

**The Chair:** If there are no further questions, may I thank both of you gentlemen very much indeed for your time this afternoon and for giving us your evidence. It is hugely appreciated. We now move on to the sixth panel.

**Examination of Witnesses**

*Harry Weber-Brown and Phillip Mind gave evidence.*

2.23 pm

**The Chair:** Welcome, gentlemen. We will now hear from Harry Weber-Brown, chief engagement officer at ZILO, and Phillip Mind, director of digital technology and innovation at UK Finance. We have until 2.50pm for this session. I now invite the witnesses to please introduce themselves to the Committee for the record, starting with Mr Weber-Brown.

***Harry Weber-Brown:*** Thank you very much. My name is Harry Weber-Brown, chief engagement officer for ZILO Technology Ltd, which is a start-up based in London. I have previously worked for the Investing and Saving Alliance. I have much experience in both smart data, which is dealt with in part 3 of the Bill, and digital identity, which relates to digital verification services in part 2.

***Phillip Mind:*** Good afternoon. I am Phillip Mind, director of digital technology and innovation at UK Finance, a trade body representing over 300 organisations in the bank and finance community. Like Harry, my expertise resides more in parts 2 and 3 of the Bill, although I have a few insights into part 1.

**Q101 Stephanie Peacock:** Good afternoon to both witnesses. I have a broad opening question. What are the main implications of the Bill's provisions for the finance sector?

***Phillip Mind:*** The banking community is supportive of the Bill, which is enabling of a digital economy. The data protection reforms reduce compliance burdens on business, which is very welcome. The provisions on digital identity are enabling, and we see digital identity as an essential utility for customers in the future. The provisions on smart data extend an open data regime to other sectors. We already have an open banking regime, and we are keen for that to extend to other sectors. It offers real opportunities in terms of innovative products and services, but we would caution the Committee that there is significant cost and complexity in those measures.

***Harry Weber-Brown:*** The Bill is key to retaining the UK's place as a hub for technical innovation, and in particular for investment in fintech. It is critical also to make sure the UK remains a global leader in data portability. Building on the work that Phillip just mentioned on open banking, which has over 7 million users among both consumers and small and medium-sized enterprises, it is critical that we make sure we are ahead of the competition.

For the financial services sector, the provisions on ID help to reduce costs for things like onboarding and reduce fraud for things like authorised push payments. It also delivers a better customer experience, so you do not have to rummage around to find your passport every time you want to set up a new account or need to verify yourself to a financial service firm.

Smart data is an opportunity for us to extend ourselves as the world leader in open finance, building on the work of not only open banking but the pensions dashboard, which is yet to be launched but is another open finance scheme. The opportunity to widen up and give consumers more control in their ability to share data is critical for the customer, the economy and the financial services industry.

**Q102 Stephanie Peacock:** That is great. You both mentioned smart data. For the benefit of the Committee, could you outline some of the progress that the banking and finance industries have made in developing smart data initiatives?

***Phillip Mind:*** In the banking industry we have open banking, which allows customers to choose and consent to allow an authorised third party provider access to their account to provide products and services—access to see the data. It also allows—again, with customer choice and consent—customers to allow a third party provider to make payments on their behalf. That has been hugely enabling. It has enabled growth in all sorts of innovative products and services and growth in fintech in the UK. As Harry mentioned, there are over 7 million active customers at the moment, but it does come with a cost; it is not a free good. Making that service available has involved cost and complexity.

In extending the provisions to other sectors through secondary legislation, it is really important that we are cognisant of the impacts and the unintended consequences. Many sectors have pre-existing data-sharing arrangements, many of which are commercial, and it is important that we understand the relative costs and benefits and how they fall among different participants in the market. My caution to the Committee and to Government is to go into those smart data schemes with eyes open.

**Q103 Stephanie Peacock:** To develop that point, do you think there are enough safeguards in the Bill to ensure that Ministers assess the commercial sense and the impact of any new smart data regimes before regulating for them?

***Phillip Mind:*** Clauses 62 and 64 make provision for the Secretary of State and Treasury to consult on smart data schemes. We think that those provisions could be strengthened. We see a need for impact assessments, cost-benefit analysis and full consultation. The Bill already allows for a post-implementation review, and we would advise that too.

***Harry Weber-Brown:*** I think the other one to call out is the pensions dashboard, which has been driven out of the Money and Pensions Service. Although it has not actually launched yet, it has brought the life assurance industry on the site to develop free access to information. The consumer can see all their pensions holdings in a single place, which will then help them to make better financial decisions.

I think my former employer, the Investing and Saving Alliance, was working on an open savings, investments and pensions scheme. Obviously, that is not mandatory, but this is where the provision for secondary legislation is absolutely imperative to ensure that you get a wide scope of firms utilising this. At the moment, it is optional, but firms are still lining up and wanting to use it. There is a commitment within the financial services industry to do this, but having the legislation in place—secondary legislation, in particular—will ensure that they all do it to the same standards, both technical and data, and have a trust framework that wraps around it. That is why it is so imperative to have smart data.

**Q104 Sir John Whittingdale:** Would you say a little about the international position? You referred to the UK's position as a leader in this field. To what extent is that the case? What are the benefits, and what is the risk to the UK's position if we do not make the changes proposed in the Bill?

***Harry Weber-Brown:*** In part 2 or part 3 of the Bill? The digital verification services or smart data?

**Sir John Whittingdale:** I will come on to digital verification. Let us focus on smart data, to begin with.

***Harry Weber-Brown:*** On that, Australia is certainly one of the leaders. The consumer has a data right under legislation that enables them to recall information from across a variety of sectors, not just financial services, and to have their information in a structured format shared with a data consumer—a third-party provider in open banking. Things are afoot. A lot of work is going on in the States, but less in Europe, interestingly. Legislation is coming through, but I think the big country to watch from our perspective is Australia and what has happened there. Theirs is a more far-reaching approach than, say, we have. That is for the smart data side.

There is a risk that if we do not extend that data right to other financial services, the consumer has a very limited view of what they can actually share. They can share their bank account details and possibly their pensions data as well, but what about their savings and investments, certainly in non-pension type wrappers? Give the consumer a full, holistic view of all their holdings and their debt as well, so that they can see their balance, as it were, and make better financial decisions. That is why we think it is so important to have part 3 of the Bill go through and for secondary legislation to follow behind it.

There is a risk that if we do not do that, the consumer has a very fragmented view. Does that mean that overseas, where it is legislated for, the consumer would have a more holistic view of everything? Would that drive investment overseas, rather than into the UK? As Phillip said, open banking has really heralded a range of fintech providers being able to consume data and provide value-added services on top of that banking data. I think it rebalances the marketplace as well.

***Phillip Mind:*** To build on Harry's remarks, I think that the real opportunity is for the UK to build a flourishing fintech industry. We have that already; open banking is actually one of our exports. Our way of doing open banking—the standards and the trust framework—has been a successful export, and it has been deployed in other jurisdictions. The opportunity around open data is to maintain that competitiveness for UK fintech when it is trading abroad.

Most of the consequences of extending beyond open banking into other smart data schemes impact UK businesses and consumers. I do not necessarily see that there is a competitiveness issue; it is bounded within the domestic economy.

**Q105 Sir John Whittingdale:** Moving on to the digital identity provisions, clearly some people are already familiar with this, but there is still a degree of suspicion. To what extent do you think that the consumer needs persuasion about the security and the benefits of digital identity services? Do you see that as being addressed by the provisions in the Bill?

***Harry Weber-Brown:*** That is a very good question. I did quite a lot of consumer research in my previous capacity, and consumers are initially quite sceptical, asking "Why are you asking me for identity details and things?" You have to explain fully why you are doing that. Certainly having Government support and things like the trust framework and a certification regime to make sure that the consumer knows whom they are dealing with when they are passing over sensitive data will help to build the trust to ensure that consumers will utilise this.

The second part to that is what types of services are built on top of the identity system. If I have the identity verified to an AML—anti-money laundering—standard for financial services, I could use it for a whole suite of other types of activity. That could be the purchase of age-restricted products, or sharing data with my independent financial adviser; it could reduce fraud in push payments, and so on. There is a whole suite of different types of services; you would not be using it just for onboarding. I think the Government support of this under digital verification services, part 2 of the Bill, is critical to make sure it happens.

It is opt-in. We are not saying to people that they have to get an identity card, which obviously is not hugely popular; but if we can demonstrate the value of having a digital identity, with support and trust—with the trust framework and certification with Government—we will not necessarily need to run a full marketing campaign to make sure that consumers use this.

Look at other territories—for example, Norway with Vipps, or Sweden's BankID. I think about 98% of the population now use ID in a digital format; it is very commonplace. It is really a question of looking at the use cases—examples of how the consumer could utilise this—and making sure they receive utility and value from the setting up and the utilisation of the ID. The ID by itself is not necessarily compelling enough; the point is what you can use it for.

***Phillip Mind:*** Trust and acceptance are key issues, and the Bill lays the legislative foundations for that. We already assert our identity digitally when we open accounts, but we do so on a one-off basis. The challenge is to go from doing so on a one-off basis to creating a digital token that is safe and secure and that allows us to reuse that digital identity. For that to work, that token has to be widely accepted, and that is a really complex strategic challenge, but the Bill lays the foundations.

We will transact digitally more and more; that is for sure. At the moment, we have a consultation, from the Treasury and the Bank of England, on a central bank digital currency. Arguably, that would benefit hugely from a reusable digital identity, but we need to be able to create the token in the right way. It could be enabling for people who have access to a smartphone but do not have a passport or driving licence; it could also build inclusion, in terms of identity. So we are very supportive of a reusable digital identity, but it is a big challenge, and the challenge is gaining trust and acceptance.

**Q106 Damian Collins:** Mr Weber-Brown, you in particular have spoken about the consumer benefits of data sharing—having a wider choice of products and services. What do you see as the principal business benefits for financial service providers? How wide would you like the scope of their access to data to be?

***Harry Weber-Brown:*** Financial services obviously rely heavily on data to be able to fashion their products accordingly and make them personal, so I think it is critical to have a smart data regime where everything is collected in a single format—what is known as an API, an application programming interface, which is a common way of securely sharing data.

Some of the other use cases from smart data that would benefit business would be things like sharing data around fact find. For example, if someone wants to instruct an independent financial adviser, could they not use this as a way of speeding up the process, rather than having to wait on letters of authority, which are written and take time? Similarly, with pension providers, if I wanted to move from one pension to another or to consolidate things, could we use the smart data to get an illustration of what impact that might have, so that before I ported it over I could see that?

For big financial services firms—well, for all of them—efficiencies are delivered because, as my colleague said, we are using digital as opposed to having to rely on manual processing. As long as the safeguards are put in place, that spawns a whole array of different types of use case, such as with regulatory reporting. If I need to report things to the regulator, could I use smart data provision to do that? That would benefit businesses. A lot of the financial services industry still relies on reporting on Excel spreadsheets and CSV files, so if we can digitise that, it would certainly make it a much more efficient economy.

**Q107 Damian Collins:** Can you understand that there might also be concerns on the consumer side about data profiling consumers based on risk? That would make a lot of sense for financial services. You have described certain financial products, but equally there are people offering loans, mortgages, insurance and things like that who will be very keen to understand more about their customers before pricing their products accordingly.

***Phillip Mind:*** A digital identity gives customers more control. One of the issues that we face at the moment when we present a passport or driving licence is that we cannot minimise the data there. There is a data minimisation opportunity and benefit.

For businesses and customers, too, identity is a key issue when we transact digitally. There are risks around profiling, but there are real opportunities around anti-fraud as well. Being absolutely clear about who we are transacting with and being able to prove incontrovertibly who we are through a safe and secure token will deliver huge benefits to the economy.

**Damian Collins:** We talked in the previous session about the undoubted benefits, which you have set out clearly. Equally, however, consumers will still want to know what sort of data about them is being used and who has access to it. For example, if a video games maker is profiling the attitudes of players to risk, in order to stimulate them with risk-and-reward opportunities within a game like Fortnite, consumers might understand how that makes their gameplay more interesting. They might consent to that, but they might not necessarily want a financial services provider to have access to that information, because it could create a picture of them that is not flattering.

***Harry Weber-Brown:*** That is a perfectly good challenge. There is a spawning part of the industry around consent dashboards. The idea there is that we put much more control in the hands of the consumer, so that they can see where they have given consent to share data and what data has been shared, while also having the right of revocation and so on. There are technical workarounds to ensure that consumers are much more empowered to control their data. Certainly the legislation supports that, but there will be the technical implementation that sits behind it to ensure that the GDPR is abided by and that the smart data will facilitate better services to consumers. The technology is the answer, but the smart data will open up the opportunity to make sure that the consumer is protected, while with things like consent dashboards they can take better control of where their data is being shared.

***Phillip Mind:*** The interesting thing about digital identity is that it creates a tether. In the future, you will be able to tether digitalised tokens such as securities or deeds to an identity in a safe way, but you could also tether consent to a digital identity, giving a customer or citizen a more holistic view of what they have consented to and where. As Harry says, for those who have real data literacy issues, we will see intermediaries offering services around consent. Those services exist in other jurisdictions.

**Damian Collins:** I think the Estonian digital ID model works in a very similar way.

**Q108 Chi Onwurah:** You have both spoken very passionately, if I may say so, about the importance of citizens being in control of their data, particularly with

*[Chi Onwurah]*

open banking. We all take very seriously our financial data and the importance of trust and empowerment in these services. Can you say how the Bill will improve trust and control for citizens, or how it should do so?

***Harry Weber-Brown:*** Part 2 of the Bill sets out the trust framework, which was being developed by the then Department for Digital, Culture, Media and Sport and which now comes under the Department for Science, Innovation and Technology. It will give certainty to the marketplace that any firm that wishes to store data—what is commonly known as an identity provider—will have to go through a certification regime. It will have to be certified against a register, which means that as a consumer I will know that I can trust that organisation because it will be following the trust framework and the policies that sit within it. That is critical.

Similarly, if we are setting up schemes with smart data we will need to make sure that the consumer is protected. That will come through in secondary legislation and the devil will be in the detail of the policies underpinning it, in a similar way to open banking and the pensions dashboard.

Further to the previous session, the other thing I would say is that we are talking on behalf of financial services, but parts 2 and 3 of the Bill also refer to other sectors: they apply equally to health, education and so on. If as a consumer I want to take more control of my data, I will want to be able to use it across multiple services and get a much more holistic view not just of my finances, but of my health information and so on.

One area that is particularly developing at the moment is the concept of self-sovereign identity, which enables me as a consumer to control my identity and take the identity provider out of the equation. I do not want to get too technical, but it involves storing my information on a blockchain and sharing my data credentials only when I need to do so—obviously it follows data minimisation. There are evolving schemes that we need to ensure the Bill caters for.

**Q109 Chi Onwurah:** Thank you very much for those points.

You mentioned data verification services. Briefly, can you help the Committee to understand who would be providing those services and who would be paying for them? You gave the example of tethering my property or other ownership. Who would be paying in that case? Would I be paying for the rest of my life to keep that data where it is? How do you see it working?

***Phillip Mind:*** Who will provide the services? There is already a growing list of verified providers. There is a current market in one-off digital identity services, and I think many of those providers would step in to the reusable digital identity market.

What is the commercial model? That is a really good question, and frankly at this point I do not have an answer. That will evolve, but within the frameworks that are set up—trust schemes, in the jargon—there will be those who provide digital identity services and those organisations that consume them, which could be retailers, financial services providers or banks. It is likely that the relying parties, the consumers, would pay the providers.

***Harry Weber-Brown:*** But not the individual consumers. If you wanted to open a bank account, and the bank was relying on identity measures provided by fintech, the bank would pay the fintech to undertake those services.

**The Chair:** We have time for a very quick question from Rupa Huq, with very quick answers.

**Q110 Dr Rupa Huq** (Ealing Central and Acton) (Lab): UK Finance's members are all the big banks—is that right?

***Phillip Mind:*** We represent more than 300 organisations in the banking and finance community. Some are big banks and some are quite small fintechs, so there is quite a spectrum.

**Q111 Dr Huq:** Okay. The dealings that I have had with you have been about the bank card phenomenon. We know that there is public mistrust in the consumer banking sector about how our data is controlled. How will you ensure that the Bill does not leave behind those people who are not online? That is what the banking hubs are aimed at, is it not? There is a whole loneliness agenda, as well as issues relating to the elderly.

**The Chair:** You have 30 seconds to answer.

***Phillip Mind:*** That is a big challenge. It is really important that people are not left behind and that they have the ability to create a kind of digital identity. As a society, we will have to work very hard to enable that. That is a responsibility that falls not on banks, but on other organisations that will help citizens to create these identities.

**The Chair:** Thank you very much indeed for your evidence this afternoon and for giving us the benefit of your time. We appreciate it.

**Examination of Witness**

*Keith Rosser gave evidence.*

2.50 pm

**The Chair:** Welcome, Mr Rosser. We have just 15 minutes, until 3.05 pm, for this session. Would you kindly introduce yourself to the Committee for the record?

***Keith Rosser:*** My name is Keith Rosser. I am the chair of the Better Hiring Institute.

**Q112 Stephanie Peacock:** Good afternoon. What are the main implications of the Bill for employers? Specifically, how will enabling greater use of a digital verification service help employers to make hiring decisions?

***Keith Rosser:*** Employers have been making hiring decisions using digital identity since 1 October, so we are a live case study. The biggest impact so far has been on the speed at which employers are able to hire staff and on the disconnection between where people live and the location of their job. For example, people in a digital identity scheme could apply for work, get a job and validate who they are without ever necessarily having to go and meet the employer. It is really important across the regions, from St Austell to Glasgow, that we

are opening up job opportunities across the UK, including in some of our urban areas—West Bromwich, Barnsley and others—where people get greater job opportunities from where they live because they are not tied to where the employer is. It has had a profound effect already.

We recently looked at a study of 70,000 hires or people going through a hiring process, and 83%—some 58,000—opted to take the digital identity route. They did it in an average time of three minutes and 30 seconds. If we compare that with having to meet an employer and go through a process to provide your physical documents, there is a saving of around a week. If we think about making UK hiring the fastest globally, which is our ambition, people can start work a week earlier and pay taxes earlier, and we are cutting waiting lists and workloads. There is a huge positive impact.

In terms of employers making those hiring decisions, technology is so much better than people at identifying whether a document is genuine and the person is who they say they are. In that case study, we found that 200 of the 70,000 people going through the process had fake documents or fraudulently obtained genuine documents. The question is, would the human eye have spotted that prior to the implementation of digital identity? I am certain that it would not have done. Digital identity is really driving the potential for UK hiring to be a shining example globally.

**Q113 Stephanie Peacock:** Do you think the provisions in the Bill will help to improve public trust in digital identities?

***Keith Rosser:*** From that 70,000 example, we have not seen evidence yet that public trust has been negatively impacted. There are some very important provisions in the Bill that have to go a long way to assuring that. One is the creation of a governance body, which we think is hugely important. There has to be a monitoring of standards within the market. It also introduces the idea of certifying companies in the market. That is key, because in this market right now 30% of DVSs—nearly one in three companies—are not certified. The provision to introduce certification is another big, important move forward.

We also found, through a survey, that we had about 25% fewer objections when a user, company or employer was working with a certified company. Those are two really important points. In terms of the provision on improving the fraud response, we think there is a real opportunity to improve what DVSs do to tackle fraud, which I will probably talk about later.

**Q114 Sir John Whittingdale:** Perhaps I could ask you to expand on that now. To what extent would you say that some providers that are not certified are not meeting the standards necessary, or in some cases even promoting fraud?

***Keith Rosser:*** I have every reason to believe that organisations not certified will not be meeting anywhere near the standards that they should be meeting under a certified scheme. That appears really clear. They certainly will not be doing as much as they need to do to tackle fraud.

My caveat here is that across the entire market, even the certified market, I think that there is a real need for us to do more to make sure that those companies are doing far more to tackle fraud, share data and work with Government. I would say that uncertified is a greater risk, certainly, but even with certified companies we must do more to make sure that they are pushed to meet the highest possible standards.

**Q115 Sir John Whittingdale:** So would you expect that as a result of the Bill, the bar to obtain certification will be higher?

***Keith Rosser:*** Yes. The requirement on DVSs to tackle fraud should be higher than it currently is.

**Q116 Damian Collins:** I want to follow on from the Minister's questions. Looking at other legislation that is going through Parliament, particularly the anti-fraud provisions in the Online Safety Bill, one of the important areas is the extent to which regulators should expect companies to have good upstream solutions in place to combat fraud. Rather than chasing every example that they come across, they need things that block it in the first place. Do you see the provisions in this Bill as being helpful? Would you expect regulators to act on that and to direct companies to use systems that are known to be safe?

***Keith Rosser:*** Absolutely. I will give a quick example relating to the Online Safety Bill and hiring, which I am talking about. If you look at people getting work online by applying through job boards or platforms, that is an uncertified, unregulated space. Ofcom recently did research, ahead of the Online Safety Bill, that found that 30% of UK adults have experienced employment scams when applying for work online, which has a major impact on access to and participation in the labour market, for many reasons.

Turning the question the other way around, we can also use that example to show that where we do have uncertified spaces, the risks are huge, and we are seeing the evidence of that. Specifically, yes, I would expect the governance body or the certification regime, or both, to really put a requirement on DVSs to do all the things you said—to have better upstream processes and better technology.

Also, I think there is a big missing space, given that we have been live with this in hiring for eight months, to provide better information to the public. At the moment, if I am a member of the public applying for a job and I need to use my digital identity, there is no information for me to look at, unless the employer—the end user—is providing me with something up front. Many do not, so I go through this process without any information about what I am doing. It is a real missed opportunity so far, but now we can right that to make sure that DVSs are providing at least basic information to the public about what to do, what not to do, what questions to ask and where to get help.

**Q117 Chi Onwurah:** Thank you very much for your evidence so far. It is going to be informative about the use of digital ID in recruitment. You said earlier that it helps to separate away from geography, which implied that the digital ID did not reference the location or the home address of the person who was being ID'd. What does the digital ID ID? Part of the reason behind that question is this: is it simply providing identification, or

*[Chi Onwurah]*

could it also be used as part of the triage process? Can that be done algorithmically, with some of the dangers that we see in algorithmic, automated decision making?

***Keith Rosser:*** Those are several really good questions. I will use an example about location from the other perspective, first of all. At the moment, Home Office policy has not caught up with digital identity, and we are addressing that. There is a real opportunity to right that. It means that one in five work seekers right now cannot use digital identity to get a job, because they do not have an in-date British or Irish passport. If you have a visa or an in-date British or Irish passport, that is fine, but if you are among the one in five people in the country who do not have an in-date passport, you cannot. Those people have to visit the premises of the employer face to face to show their documents, or post their original documents across the UK.

This has really created a second-class work seeker. There are real dangers here, such as that an employer might decide to choose person one because they can hire them a week faster than person two. There is a real issue about this location problem. Digital identity could sever location to allow people more opportunities to work remotely across the UK.

There were really good questions about other information. The Bill has a provision for other data sharing. Again, there is the potential and the opportunity here to make UK hiring the fastest globally by linking other datasets such as HMRC payroll data. Rather than looking at a CV and wondering whether the person really worked in those places, the HMRC data could just confirm that they were employed by those companies.

There is a real opportunity to speed up the verification but, as I want to acknowledge and as you have referred to, there is certainly also a risk. Part of our mission is to make UK hiring fairer, not just faster and safer. I want to caution against going to a degree of artificial intelligence algorithmic-based hiring, where someone is not actually ever in front of a human, whether by Teams video or in person, and a robot is basically assessing their suitability for a job. We have those risks and would have them anyway without this Bill. It is really important as we go forward that we make sure we build in provisions somewhere to ensure that hiring remains a human-on-human activity in some respects, not a completely AI-based process.

**The Chair:** Mr Rosser, thank you very much indeed for your evidence this afternoon. We are grateful for your time, sir.

**Examination of Witnesses**

*Helen Hitching and Aimee Reed gave evidence.*

3.1 pm

**The Chair:** Welcome, ladies. We have until 3.30 pm for this session. Will the witnesses please be kind enough to introduce themselves to the Committee for the record? Let us start with Helen Hitching.

***Helen Hitching:*** Good afternoon. I am Helen Hitching, Chief Data Officer for the National Crime Agency, and this is my first time in front of a Committee.

**The Chair:** Welcome and thank you. Aimee Reed?

***Aimee Reed:*** Hello, everybody. This is also my first appearance in front of a Bill Committee. I am the Director of Data at the Metropolitan Police Service. For my sins, I also volunteer to lead all 43 forces on data; I am chair of the national police data board. I am here today in that capacity as well.

**Q118 Stephanie Peacock:** You are both very welcome. My first question is to Aimee. Currently, police are required by section 62 of the Data Protection Act 2018 to log their justification for accessing specific data records; this Bill, of course, changes that. How time consuming is that requirement currently for officers?

***Aimee Reed:*** It is a big requirement across all 43 forces, largely because, as I am sure you are aware, we are operating on various aged systems. Many of the technology systems across the policing sector do not have the capacity to log section 62 requirements, so police officers are having to record extra justification in spreadsheets alongside the searches and release of information that they deliver. So the requirement is a considerable burden across all the forces.

**Q119 Stephanie Peacock:** Helen, how, if at all, will listing as a recognised legitimate interest

"detecting, investigating or preventing crime",

to quote the new definition, aid the tackling of serious crime in the UK?

***Helen Hitching:*** Sorry—could you repeat that?

**Stephanie Peacock:** Sure. My understanding of the legislation in front of us is that if the Bill becomes law,

"detecting, investigating or preventing crime"

will be listed as a recognised legitimate interest and therefore be subject to separate, or slightly amended, data rules. How will that change help tackle serious crime in the UK?

***Helen Hitching:*** I think it will bring a level of simplicity across the data protection environment and make sure that we can share data with our policing colleagues and other services in a more appropriate way. It will make the whole environment less complex.

**Q120 Stephanie Peacock:** I have a connected but slightly separate question. Would being able to apply for a joint designation notice with the intelligence services aid competent authorities in targeting serious and organised crime, and if so, how?

***Helen Hitching:*** Yes, it will aid it. Again, it brings in the ability to put the data protection framework on the same level, so we can share data in an easier fashion and make it less complex.

**Q121 Sir John Whittingdale:** Can you say a little bit more about the implications of personal data sharing between countries, the extent to which that might lead to a lowering of standards of protection and how we safeguard against that?

***Helen Hitching:*** The agency does not believe that those safeguards will be lowered. We will still not be able to share data internationally with countries that do not have the same standards that are met by the UK. It

will provide greater clarity about which regimes should be used and at which point. The standards will not reduce.

**Q122 Sir John Whittingdale:** You need to be satisfied that the third country maintains the same level of data protection standards that exists in the UK. To what extent has that been an impediment for data sharing?

***Helen Hitching:*** The agency has had to undertake a test to make sure that there is adequate or, essentially, equivalent protection. That standard is now changing to "not materially lower", so it will be a lot easier to understand where those protection levels are the same as or not materially lower than the UK's. It will be simplified a lot.

**Q123 Sir John Whittingdale:** On a separate issue, at the moment we have a range of bodies responsible for different aspects of surveillance, such as the Biometrics Commissioner, the Investigatory Powers Commissioner and the Surveillance Camera Commissioner. Those are being brought together into either the Information Commissioner or the Investigatory Powers Commissioner. To what extent do you think that will improve the overall oversight of surveillance?

***Aimee Reed:*** Policing thinks that that will significantly simplify things. It will not reduce the level of oversight and scrutiny that will be placed upon us, which is the right thing to do. In terms of the simplicity of that and the regimes that we are under, we are very supportive of that change.

***Helen Hitching:*** Likewise, we are supportive and welcome the simplification. We do note, however, that the Biometrics Commissioner currently has a keen focus on developing technology in a legal manner and consults with the public. We would ask that there remains a focus on that oversight of biometrics, to assure the public that that work remains a priority once the regulation of biometrics transfers to the Information Commissioner's Office and to make sure that that focus is retained.

**Q124 Damian Collins:** How easy do you find it to gather data as part of investigations at the moment, particularly if you are working with companies that provide services to individuals? Do you think the provisions in the Bill will make that any easier?

***Aimee Reed:*** On balance, it will make things easier. We are retaining the very different sections of the Act under which different organisations operate, and the sections that look to improve joint working across part 3 and part 4 agencies are very welcome. At the moment that is not about simplifying the relationships between those in, say, part 2 and part 3, albeit data sharing is entirely possible. In essence, it is going to get simpler and easier to share data, but without losing any of the safeguards.

**Q125 Damian Collins:** In terms of criminal investigations, practically how easy is it to get hold of data and information that you consider to be important, particularly if it is from private companies?

***Aimee Reed:*** It is not as easy as we would like it to be, and provision is not made in the Bill to make that easier. There are some discussions about it going into the Online Safety Bill and other areas. It could be easier. We would push harder in the future, but at the moment, getting parity across the other areas and around national security is a focus that we welcome.

***Helen Hitching:*** I want to pick up on the fact that safeguards are not reducing. It is key that the agency notes the point that our safeguards are not being lowered because of this.

**Q126 Mark Eastwood** (Dewsbury) (Con): I have been on the parliamentary police and fire service scheme, so I have spent a lot of time with the police. One of the big frustrations from the police's point of view is the lack of free flow of information, particularly when it concerns charging decisions, along with redaction, which potentially causes some antagonism between the two. I know this is not strictly covered in the Bill, but would it be beneficial to both parties if you were able to share unredacted information before a charging decision is made?

***Aimee Reed:*** I will answer that in respect of where we are now in national policing. It would be of considerable benefit if the guidance was clearer that we could share information without having to redact it, certainly pre-charge, to enable better and easier charging decisions—to be honest—within the Crown Prosecution Service. It would also reduce the current burden on officers: you can think about the volume of data they have to hand over, and it can be video, audio, transcripts—it is not just witness statements, as it used to be 20 or 30 years ago. Reducing that burden would be significant for frontline officers and unleash them to be able to do other things.

**Q127 Mark Eastwood:** So it would be an advantage for the Government to look into including that.

***Aimee Reed:*** It certainly would. It is not that we cannot do that now; I just think the guidance could be clearer. It would put it into sharper relief if we could release that burden from policing to the CPS and the CPS felt confident that that was within the rules.

***Helen Hitching:*** The agency agrees with that—there would be the same impact.

**Q128 Chi Onwurah:** I think you implied that there was data that you would like to have access to but currently do not have access to. Can you elaborate on what data you do not have access to in terms of data sharing and the barriers? What would be helpful for investigations?

***Aimee Reed:*** It is not so much about specific datasets; it is about synchronisation and the speed with which you can exchange data that enables you to make better decisions. Because the Data Protection Act is split into three parts, and law enforcement quite rightly has a section all of its own, you cannot utilise data analytics across each of the parts. Does that make sense? If we wanted to do something with Driver and Vehicle Licensing Agency data and automatic number plate recognition data, we could not join together those two large datasets to enable mass analysis because there would be privacy rights considerations. If want to search datasets from other parts of that Act, we have to do that in quite a convoluted administrative way that perhaps we can share within law enforcement. It is more about the speed of exchange.

**Q129 Chi Onwurah:** Is it about the speed of exchange with other Government agencies or with local government agencies?

***Aimee Reed:*** It is more with our local partners. I am sure that our partners would say they are equally frustrated by the speed at which they can get data from the police in large datasets to enable them to make better decisions in their local authorities. That is just how that Act was constructed, and it will remain so. The recent ICO guidance on sharing has made that simpler, but this realm of the Bill will not make that synchronisation available to us.

**Q130 Chi Onwurah:** Do you think it should be available to you? Are there reasons why it is not available to you?

***Aimee Reed:*** It is about getting right the balance between what we do with people's personal data and how the public would perceive the use of that data. If we just had a huge pot where we put everybody's data, there would be real concerns about that. I am not suggesting for a second that the police want a huge pot of everybody's data, but that is where you have to get the balance right between knowing what you have and sharing it for the right purpose and for the reason you collected it in the first place.

**Q131 Chi Onwurah:** Just to follow up on the questions about the different types of regulation, do you feel that the balance has been struck appropriately when it comes to biometric data, particularly for facial recognition, for example?

***Helen Hitching:*** Sorry—could you repeat that?

**Chi Onwurah:** Has the balance between sharing and the regulation of biometric data, particularly facial recognition data, been struck in the right way?

***Helen Hitching:*** I do not think facial recognition data is captured.

***Aimee Reed:*** On facial recognition, given that we have deployed it—very high profile—I think that the balance is right. We have learned a lot from the South Wales judgment and from our own technical deployments. The Bill will also highlight how other biometric data should be managed, creating parity and an environment where biometric data that we do not yet have access to or use of is future-proofed in the legislation. That is really welcome.

**Q132 Rebecca Long Bailey:** Helen, you mentioned that you are broadly supportive of the abolition of the Biometrics Commissioner and the Surveillance Camera Commissioner, but that that abolition will not reduce the existing level of oversight. Now seems to be the time to request additional resources if you did not feel that the new commissioners would be adequately resourced, so do you have confidence that the Investigatory Powers Commissioner has sufficient resources and expertise to take on the functions it has to? Similarly, does the Information Commissioner have sufficient resources and expertise to oversee regulation in this area?

***Helen Hitching:*** It is difficult for the agency to comment on another organisation's resources and capabilities. That question should probably be posed directly to them. The Information Commissioner's Office already deploys resources on issues related to law enforcement data processing, including the publication of guidance. From a biometrics perspective, the casework is moving to the IPC, so from a resourcing perspective I think it would have adequate casework provision and expertise.

***Aimee Reed:*** I echo the comments about expertise, particularly of the Investigatory Powers Commissioner. I think that the expertise exists but, like Helen, whether it has enough resources to cope with the casework I presume is a demand assessment that it will do in response to the Bill.

**Q133 Rebecca Long Bailey:** I have a final question for you, Aimee. There are concerns, particularly given that the Information Commissioner's Office 2021 data protection audit report gave an assurance rating of "limited" to the Met's policies on records management. How can you reassure the public, given that there will be such an expansion of powers in the area, that the Met will not receive a similar report over the next 12 months?

***Aimee Reed:*** That is a very topical question today. The first thing to say is that I am not sure I agree that this is a large expansion of our access to personal data; I think it is a simplification of the understanding of what we can do as a law enforcement body. All the same safeguards and all the same clear water will be in place between the different parts of the Act.

We did indeed get a "limited" rating on records management, but as I am sure you are aware, we were assessed on three areas, and we got the second highest grading in the other two: the governance and accountability of our management data; and our information risk management. They came out higher.

What have we done since 2021? We have done quite a lot to improve the physical and digital records management, with greater focus on understanding what data we hold and whether we should still hold it, starting a review, retain and deletion regime. We now have an information asset register and a ROPA—record of processing activities. The previous commissioner, Cressida Dick, invested a significant amount in data management and a data office, the first in UK policing. The new commissioner, as I am sure you have seen, is very committed to putting data at the heart of his mission, too. We have already done quite a lot.

The Bill will simplify how we are able to talk to the public about what we are doing with their data, while also reassuring them about how we use it. We are in a very different place from where we were 12 months ago; in another 12 months, it will be even more significantly improved. We have just worked with the Open Data Institute to improve how open we will be with our data to the public and partners in future, giving more to enable them to hold us to account. I am already confident that we would not get a rating like that again in records management, just based on the year's review we have had from the ICO about where we have got to.

**Q134 Rebecca Long Bailey:** Similarly, now that you have authority over all forces across the UK, I have the same question regarding each of them: are you content that they are equipped and resourced adequately to meet data protection requirements, given that there is such an expansion?

***Aimee Reed:*** I wish I had authority across them. I represent—that is a better way of describing what I do. Am I confident that law enforcement in general has the right investment in this space, across all forces? No, I am not. That is what I am working hard to build with Chief Constable Jo Farrell, who leads in this area for all

forces on the DDaT approach. Am I more confident that forces really getting investment in this space is necessary? Absolutely.

**Q135 Rebecca Long Bailey:** In terms of additional resources, are there any specific figures or requirements that you could point the Government towards at this stage?

***Aimee Reed:*** In line with our own DDaT framework, we are working with the Home Office and other ministerial bodies on what good looks like and how much is enough. I am not sure that anybody has the answer to that question yet, but we are certainly working on it with the Home Office.

**The Chair:** Ladies, thank you very much indeed for your time this afternoon. We will let you get back to your crime fighting.

**Examination of Witnesses**

*Andrew Pakes and Mary Towers gave evidence.*

3.21 pm

**The Chair:** We now come to our ninth panel. We welcome Andrew Pakes, who is director of communications and research at Prospect, and Mary Towers, who is the policy officer at the Trades Union Congress. We have until 3.55 for this session. I invite the witnesses to introduce themselves to the Committee for the record—ladies first.

***Mary Towers:*** Hi, and thanks very much for inviting the TUC to give evidence today. My name is Mary Towers. I am an employment rights policy officer at the TUC, and I have been leading a project at the TUC looking at the use of AI in the employment relationship for the past couple of years.

***Andrew Pakes:*** Hello, everyone. Thank you for inviting Prospect to give evidence today. My name is Andrew Pakes. I am one of the deputy general secretaries and the research lead for Prospect union, which represents scientific, technical and professional workers. I am also a member of the OECD's AI expert panel, representing trade unions.

**Q136 Stephanie Peacock:** Good afternoon to you both; you are very welcome. My first question is to Andrew. Obviously, the nature of work has changed significantly over the past few decades, particularly in the last decade. What impact has technology, particularly the rise of automated decision making and automated performance management, had on the workplace?

***Andrew Pakes:*** We were already seeing a huge change in the use of digital technology prior to the pandemic. The pandemic itself, not least through all the means that have kept many of us working from home, has transformed that. Our approach as a trade union is to embrace technology. We believe that our economy and the jobs our members do can be made better and more productive through the good deployment of technology to improve jobs.

We also think there is a downside to it all. Everything that needs to be risked and balanced is in that. Alongside the advance in innovation and technology that has brought benefits to the UK, we have seen a rise in the darker or less savoury side of that, which is namely the rise of surveillance software; the ability of software to follow us, including while working from home, and to micromanage us and track people; and the use of technology in performance management—the so-called people analytics or HR management, which is largely an unregulated area.

If you ask me which legislation this should sit in, I would probably say an employment-type Bill, but this is the legislation we have and the Government's choice. We would definitely like to see checks and balances at least retained in the new legislation compared with GDPR, but maybe they should be enhanced to ensure that there is some form of social partnership and that working people have a say over how technology is introduced and implemented in their workspaces.

**Q137 Stephanie Peacock:** That makes sense. You mentioned the changes since the pandemic. How do you think those changes have impacted on the right to privacy and the right to a work-life balance? I presume that has shifted since the pandemic.

***Andrew Pakes:*** There is increasing evidence that while technology has allowed many of us to remain connected to our workspaces—many of us can now take our work anywhere—the downside is that our work can follow us everywhere. It is about the balance of digital disconnection and the ability to switch off from work. I am probably preaching to the wrong crowd, because MPs are constantly on their phones and other technology, but many of us are able to put that away, or should do, because we are contracted workers and have a different relationship with our workplace in terms of how that balance is struck. We very much focus on wellbeing and on information and consultation, ensuring that people are aware of the information that is collected on us.

One of the troubling factors that we and the TUC have picked up is that consistently, in opinion polls and research that is done, working people do not have confidence or knowledge about what level of data is being collected and used on them. When we see the increasing power of technology through AI and automated decisions, anxiety in the workplace is best foiled by transparency, in the first place, and, we would obviously argue, a level of social partnership and negotiation over how technology is introduced.

**Q138 Stephanie Peacock:** What effect do you believe the new rules in the Bill on automated decision making will have on workers? I think you have alluded to this, but would you like to see greater protections in place?

***Andrew Pakes:*** Absolutely. What strikes me about the legislation you are considering is that just about all our major competitors—who are more productive and more advanced, often in innovation, including the United States—are choosing a path of greater scrutiny and accountability for AI and automated decision making. There is a concern that in this legislation we are taking an alternative path that makes us stand out in the international economy, which is about diluting existing protections we have within GDPR to a lower level. That raises concerns.

We have particular concerns about automated technology, but also about the clauses on the reduction of powers around data protection impact assessments. We think

the risk is that the legislation could open the back door to the increase in dodgy surveillance and other forms of software coming into the UK market. I am worried about that for two reasons: first, because of the impact it has on individual workers and what is happening there; and secondly, because most of this technology—we have been part of a project that has tracked over 500 different surveillance software products currently on the international market—is designed largely for a US or Chinese market, with little knowledge of how it is being done.

What we know through ensuring consultation on the existing DPIA arrangements is that there is a break in the current rules that enables or ensures that employers have a consultation and check where their products are taking their data from and what they have stored. Diluting that risks ensuring that we are not sure where that data is being used and we are not sure of the power of this technology, and working people then end up with a worse deal than they currently have.

**Q139 Stephanie Peacock:** I have a couple of questions for Mary Towers. Do you think that the changes in the Bill will do anything to improve the collective rights of workers? If not, what sort of mechanisms would you like to see in place to give workers a method of redress collectively?

***Mary Towers:*** On the contrary, we would say that the Bill in fact reduces the collective rights of workers, particularly in relation to data protection impact assessments. As Andrew has mentioned, at the moment the right to a data protection impact assessment involves an obligation on an employer to consult with workers or their representatives. That is an absolutely key tool for trade unions to ensure that worker voice is represented in the path of the introduction of new technologies at work. Also, at the moment, missing from the Bill is the ability of trade unions to act as representatives for data subjects in a collective way. We say that that, too, is missing, could be added and would be an important role that unions could take on.

Another aspect missing from the Bill, which we say is a hugely missed opportunity, is a potential right that workers could have to have an equal right to their data that matches the right employers have over worker data. Once workers had that right, they could then collectivise their own data, which would enable them, for example, to pick up on any discriminatory patterns at work or pick up any problems with equal pay or the gender pay gap. We say that that right to collectivise data and redress the imbalance of power over data at work is really important.

The Bill misses entirely the opportunity to introduce those kinds of concepts, which are actually vital in the modern workplace, where data is everything. Data is about control; data is about influence; data is the route that workers have to establish fair conditions at work. Without that influence and control, there is a risk that only one set of interests is represented through the use of technology at work, and that technology at work, rather than being used to improve the world of work, is used to intensify work to an unsustainable level.

**Q140 Stephanie Peacock:** In that answer, you highlighted the imbalance between employers and workers. Correct me if I am wrong, but you said that data protection impact assessments are particularly valuable to both trade unions and the collective workforce. Do you have any specific examples of this consultation tool being used successfully?

***Mary Towers:*** Yes. This is something that Andrew's union, Prospect, has been really active in. It has produced some absolutely brilliant guidance that looks in detail at the importance of the process of data protection impact assessments and rolled out training for its trade union reps. Again, several of our other affiliates have undertaken that really important work, which is then being rolled out into the workplace to enable reps to make good use of that process.

I will, however, add the caveat that I understand from our affiliates that there is a very low level of awareness among employers about that obligation, about the importance of that process and about exactly what it involves. So a really important piece of awareness-raising work needs to be done there. We say it is vital to build on the existing rights in the UK GDPR, not dilute or remove them.

**Q141 Stephanie Peacock:** What impact would the Bill have on workers by taking away this tool or watering down the DPIAs into assessments of high risk, especially given that earlier today, before this Committee, the Information Commissioner himself raised concerns about the lack of clarity on what will count as high-risk processing? That question is to either of you, briefly. I have one more and then I will let someone else come in.

***Andrew Pakes:*** We would assert that under the law of GDPR, high risk in the legislation is, I think, in recital 39. I will correct that if I picked the wrong one. It talks about high risk as being decisions that can make material or non-material impact on people. If we now have software and algorithms or automated decisions that can hire and fire us—we have examples of that—and can decide who deserves a promotion or who can be disciplined, if that information can now be used to track individuals and decide whether someone is a good or bad worker, we would assert that that is a high risk. Anything that can actually affect both your standing in your workspace or your contractual relationship, which is essentially what employment is, or which has an impact on the trust and confidence the employer has in you and, equally, your trust and confidence back in the employer, that is a very clear definition of high risk.

What is important about the existing UK GDPR is that it recognises the nature of high risk but, secondarily, it recognises that data subjects themselves must be consulted and involved either directly or, where that is not practicable, through their representatives. Our worry is that the legislation that is tabled now dilutes that and opens up risk to bad practice.

**Q142 Stephanie Peacock:** Thank you. This is my final question. Does the Bill offer enough detail on the new threshold for charging or refusing a subject access request that is either "vexatious or excessive" to assure workers that they will still be able to access their personal records from an employer when making a good-faith request?

***Mary Towers:*** The right to a data subject access request—again, like the DPIAs—is an absolutely crucial tool for trade unions in terms of establishing transparency over how their data is being used. Really, it provides a

route for workers and unions to get information about what is going on in the workplace, how technologies operate and how they are operating in relation to individuals. It is an vital tool for trade unions.

What we are concerned about is that the new test specified in the Bill will provide employers with very broad discretion to decide when they do not have to comply with a data subject access request. The use of the term "vexatious or excessive" is a potential barrier to providing the right to an access request and provides employers with a lot of scope to say, for example, "Well, look, you have made a request several times. Now, we are going to say no." However, there may be perfectly valid reasons why a worker might make several data subject access requests in a row. One set of information that is revealed may then lead a worker to conclude that they need to make a different type of access request.

We say that it is really vital to preserve and protect the right for workers to access information. Transparency as a principle is something that, again, goes to really important issues. For example, if there is discriminatory operation of a technology at work, how does a worker get information about that technology and about how the algorithm is operating? Data subject access requests are a key way of doing that.

**Q143 Sir John Whittingdale:** May I ask a relatively simple question? Obviously your concern is the protection of workers' rights, and safeguards against discrimination and other potential adverse consequences of technology. We will debate the provisions of the Bill in those areas in the coming weeks—I suspect at some length—but would you nevertheless accept that the overall impact of the legislation, if we get this right, will be beneficial to your members in terms of the promotion of growth and potential future job opportunities?

***Andrew Pakes:*** "If we get this right" is doing a lot of heavy lifting there; I will leave it to Members to decide the balance. That should be the goal. There is a wonderful phrase from the Swedish trade union movement that I have cited before: "Workers should not be scared of the new machines; they should be scared of the old ones." There are no jobs, there is no prosperity and there is no future for the kind of society that our members want Britain to be that does not involve innovation and the use of new technology.

The speed at which technology is now changing and the power of this technology compared with previous periods of economic change make us believe that there has to be a good, robust discussion about the balances of checks and balances in the process. We have seen in larger society—whether through A-level results, the Post Office or other things—that the detriment is significant on the individuals impacted if legislators get that balance wrong. I agree with the big principle and I will leave you to debate that, but we would certainly urge that checks and balances need to be balanced, not one-sided.

***Mary Towers:*** Why does respect for fundamental rights have to be in direct conflict with growth and innovation? There is not necessarily any conflict there. Indeed, in a workplace where people are respected, have dignity at work and are working in a healthy way, that can only be beneficial for productivity and growth.

**Q144 Damian Collins:** I have been listening carefully to what you have been saying and it strikes me that there are two issues: the use of technology in the general workplace, and the rights of workers who work through technology to do their jobs. In the workplace itself, data gathering and analysis has always existed to some extent. If we were having this conversation in the 1960s, we would have been talking about people doing time-motion studies of people in factories to work out what efficiency looked like. Is your concern in respect of a general working environment that employers are transparent about what sort of data they gather and how they use it?

***Andrew Pakes:*** That is the first base. The power of technology is changing so quickly, and the informal conversations we have every day with employers suggest that many of them are wrestling with the same questions that we are. If we get this legislation right, it is a win-win when it comes to the question of how we introduce technology in workspaces.

You are right to identify the changing nature of work. We would also identify people analytics, or the use of digital technology to manage people. How we get that right is about the balance: how do you do it without micromanaging, without invading privacy, without using technology to make decisions without—this is a horrible phrase, but it is essentially about accountability—humans in the loop? Good legislation in this area should promote innovation, but it should also have due regard to balancing how you manage risks and reduce harms. That is the element that we want to make sure comes through in the legislation in its final form.

**Q145 Damian Collins:** So you do not have an in-principle objection to the use of technology to monitor the efficiency, output and performance of employees within a working environment, but you think it needs to be based on agreed criteria—that employers need to be transparent about how they are gathering data and what they are using it for.

***Andrew Pakes:*** Absolutely. Let me give you a quick example of one piece of technology that we have negotiated in some areas: GPS tracking. It might be old technology, compared with many things that you are looking at. We represent frontline workers who often work alone, outside, or in spaces where their work could be risky. If those people cannot answer their radio or phone, it is in the legitimate interests of all of us to see where they are, in case they have had an accident or are in a dangerous situation. We can see a purpose to that technology. In negotiation with employers, we have often said, "This is good technology for keeping people safe, but we are not happy with it being used in performance reviews." We are not happy with people saying, "I am sorry, Mr Collins, but you seem to spend a lot of time in the same café each lunch time."

The issue is not the technology, but its application. Technology that is used to increase safety is very good, but the risk is that it will be used to performance-manage people; employers may say, "You are not doing enough visits," "You aren't working fast enough," or, "You don't drive fast enough between jobs." We need balance and control, as opposed to ruling out technology that can keep people safe and well.

**Q146 Damian Collins:** For some people, their job is done through technology. Take a gig economy worker working for a delivery company. Do you have concerns about how app developers design their systems and

*[Damian Collins]*

their relationship to the worker? For example, you may work for a company that does not pay you for your waiting time. You are not working contracted hours; you are working in the gig economy, on a "turn up and get paid" basis. The system may have been designed to favour people who are always on the app and always ready for work, even if they are not being paid for that, over people who log on only at particular times. The app developer may not be very transparent about that, because they do not want to be named and shamed for treating their workers that way. Good and bad employers would say that there are people working to different standards, but do you feel that there is still a lack of transparency in the gig economy about how different apps process and use data, and the impact that has on the day-to-day working life of the people who use those apps?

***Andrew Pakes:*** From my perspective, yes.

***Mary Towers:*** The TUC has red lines relating to the use of these types of technologies. One is that we simply should not have technologies at work that are not transparent and that operate in a way that people do not understand. The principle of explainability is really important to us. People need to understand when the technologies are operating, and how they operate in relation to them. On top of that, it is absolutely vital that discriminatory data processing does not take place. The example that you gave from the gig economy is potentially of a discriminatory pay calculation—of an algorithm that might be calculating different rates of pay for individuals who are carrying out exactly the same work. The algorithm is potentially replicating existing inequalities in pay that are rooted in gender or race.

**Q147 Damian Collins:** The issue is not different rates of pay per task, but the amount of paid work that someone might get within a period.

***Mary Towers:*** Yes. Drivers are a good example. People drive a certain distance to pick people up or deliver items. Even when the driving time is exactly the same, people may be paid different rates, because the algorithm will have worked out how long certain groups of people are likely to wait before they accept a gig, for example. I emphasise that, in our view, those sorts of issues are not restricted to the gig economy; they spread way beyond it, into what one might consider to be the far more traditional professions. That is where our red lines are. They relate to transparency, explainability, non-discrimination and, critically, worker and union involvement at each stage of the AI value chain, including in the development of that type of app—you mentioned development. Unless the worker voice is heard at development stage, the likelihood is that worker concerns, needs and interests will not be met by the technology. It is a vital principle to us that there be involvement of workers and unions at each stage of the AI value chain—in development, application and use.

**Q148 Chi Onwurah:** Welcome to both of you. Apologies for my misuse of my own technology earlier.

The Minister talked about the need for growth, which has been sadly lacking in our economy for the last 13 years. Obviously, technology can make huge improvements to productivity for those in the workforce. Mr Pakes, as someone whose members are involved in technology, scientific and IT organisations, I wonder whether you would agree with this, which comes from my experience in the diffusion of technology. Is it possible to get the best from technology in an organisation or company without the people who will be using it, or the people on whom it will be used, being an active part of that diffusion of technology, and understanding and participating in its use?

***Andrew Pakes:*** Absolutely. That has always been how productivity has improved or changed, in effect, the shop floor. If you are asking, "What problems are you using technology to solve?", it may well be a question better asked by the people delivering the product or service than necessarily the vendor selling the software, whether that is old or new technology. I encourage the Committee to look at the strong evidence among our competitors who rate higher, in terms of productivity and innovation, than the UK, where higher levels of automation in the economy are matched by higher levels of worker participation. Unions are the most common form, but often it can be works councils or small businesses in terms of co-design and collaboration. We see that social partnership model of the doers, who identify and solve problems, being the people who do that.

We have good examples. We represent members in the nuclear sector who are involved in fusion, small modular reactors or other technology, where the employer-union relationship is critical to the UK's intellectual property and the drive to make those successful industries. In the motor industry and other places where the UK has been successful, we can see that that sense of social partnership has been there. We have examples around using AI or the monitoring of conversations or voices. Again, I mentioned GPS tracking, but in safety-critical environments, where our members want to be kept safe, they know that technology can help them. Having that conversation between the workforce and the employer can come up with a solution that is not only good for our members, because they stay safe and understand what the safety regime is, but good for the employer, because days are not lost through illness or accidents. For me, that sense of using legislation like this to underpin good work conversations in the data setting is what the mission of this Bill should be about.

**Q149 Chi Onwurah:** In terms of data sharing, should there be provisions in the Bill to ensure that workers can give free and informed consent to the sharing of their data, or will the asymmetry of the relationship in the employment contract make that challenging?

***Andrew Pakes:*** We think there should be a higher bar, because of the contractual nature. Whether it is self-employed workers contracting for a piece of work or an employment relationship, there is a fundamental difference in our view between my individual choice to go online and enter my data into a shop, because I want to be kept appraised of when the latest product is coming out—it is my free choice to do that—and my being able to consent in an employment relationship about how my data is used. As Mary said, the foundation stone has to be transparency on information in the first place. Beyond that, there should be negotiation to understand how that data is used.

The critical point for us is that most companies in the UK are not of a size where they will be developing their own AI products—very few will be; we can probably name a couple of them. Most companies using automated decisions or AI will be purchasing that from a global marketplace. We hope many of them will be within certain settings, but we know that the leaders in this tend to be the Chinese market and the US market, where they have different standards and a range of other things. Ensuring that we have UK legislation that protects that level of consent and that redresses that power balance between workers and employers is a critical foundation to ensuring that we get this right at an enterprise level.

**Q150 Chi Onwurah:** Have you identified any provisions to achieve that in the Bill as it stands?

***Andrew Pakes:*** We would like to see more. We are worried that the current legislation, because of things such as DPIAs, drops that level of standards, which means that the UK could end up trading on a lower standard than other countries, and that worries us.

***Mary Towers:*** We are also concerned about the change to the test for international data transfers, which might make the requirements less restrictive. There is a change from adequacy to a more risk-based assessment process in terms of international data transfers. Again, we have very similar concerns to Andrew about the use of technologies rooted in international companies and the inevitable international transfers of data, and workers essentially losing control over and knowledge of what is happening with their data beyond the workplace.

In addition, I would also like to make a point about the importance of transparency of source code, and the importance of ensuring that international trade deals do not restrict that transparency, meaning that workers cannot access information about source code once data and AI-powered tools are rooted in other countries.

**Q151 Mark Eastwood:** I would like to declare, again, that I am a member of Prospect, and therefore I have a bit of skin in the game on this one. You mentioned GPS and surveillance technology. Very quickly, could you give me an idea of the current scale of that? Are the majority of employers going down this route? If this Bill is pushed through, could you give me an idea of how usage could increase or decrease, depending on how you see the outcome of the Bill?

***Mary Towers:*** I will give my statistics very quickly. Our polling revealed that approximately 60% of workers perceived that some form of monitoring was taking place in their workplace. The CEO of IBM told Bloomberg last week that 30% of non-customer facing roles, including HR functions, could be replaced by AI and automation in the next five years.

A recent report from the European Commission's Joint Research Centre—the "Science for Policy" report on the platformatisation of work—found that 20% of German people and 35% of Spanish people are subject to algorithmic management systems at the moment. Although that is obviously not UK-based, it gives you a very recent insight on the extent of algorithmic management across Europe.

***Andrew Pakes:*** And that matches our data. Around a third of our members say that they are subject to some form of digital monitoring or tracking. That has grown, particularly with the rise of hybrid and flexible working, which we are in favour of. This is a problem we wish to solve, rather than something to stop, in terms of getting it right.

Over the past two years, we have increasingly seen people being performance managed or disciplined based on data collected from them, whether that is from checking in and out of buildings, their use of emails, or not being in the right place based on tracking software. None of the balances we want should restrict the legitimate right of managers to manage, but there needs to be a balance within that. We know that using this software incorrectly can micromanage people in a way that is bad for their wellbeing.

The big international example, which I will give very quickly, is that if you look at a product like Microsoft—a global product—employers will buy it. My work computer has Office 365 on it. Employers get it on day one. The trouble with these big products is that, over time, they add new products and services. There was an example where Microsoft did bring in a productivity score, which could tell managers how productive and busy their teams were. They rowed back on that, but we know that with these big, global software projects—this is the point of DPIAs—it is not just a matter of consultation on day one.

The importance of DPIAs is that they stipulate that there must be regular reviews, because we know that the power of this technology transforms quickly. The danger is that we make life miserable for people who are good, productive workers and cause more problems for employers. It would be better for all of us to solve it through good legislation than to arm up the lawyers and solve it through the courts.

**The Chair:** I am afraid that we are subject to chronological monitoring, so we must bring this session to an end. I thank our two representatives very much indeed for their evidence this afternoon; we are grateful for your time. We will now move on to our 10th panel.

**Examination of Witnesses**

*Alexandra Sinclair, Ms Laura Irvine and Jacob Smith gave evidence.*

3.55 pm

**The Chair:** Welcome to the witnesses in our 10th panel. Thank you for your time this afternoon. We will hear from Alexandra Sinclair, a research fellow at the Public Law Project; Laura Irvine, via Zoom, the convener of the privacy law sub-committee at the Law Society of Scotland; and Jacob Smith, the UK accountability team leader at Rights and Security International. We have until 4.25 pm for this session. Would the witnesses please be kind enough to introduce themselves to the Committee for the record, starting with those in the room?

***Alexandra Sinclair:*** Thank you to the Committee for inviting me. My name is Alexandra Sinclair and I am a research fellow at the Public Law Project. The Public Law Project is an access to justice charity. We help people to seek redress for unfair or unlawful decisions made by public authorities. I am also a doctoral researcher at the London School of Economics where my research focuses on automated decision making.

***Jacob Smith:*** My name is Jacob Smith. I am the UK accountability team leader at Rights and Security International, a London-based charity aimed at the intersection between national security and human rights, which tries to ensure that when Governments take pledges in the name of national security, they comply with human rights. I am also an associate lecturer in international law, privacy and data governance at the University of Surrey.

***Ms Irvine:*** I am Laura Irvine. I am the convener of the privacy law sub-committee at the Law Society of Scotland. My day job is head of regulatory law at Davidson Chalmers Stewart—a Scotland-based law firm. I have been working in the field of data protection law for the past 10 years, so pre-GDPR and obviously, more recently, in a post-GDPR world.

**The Chair:** Thank you. You are all very welcome.

**Q152 Stephanie Peacock:** My first question is to Alexandra. What would the benefit be to the general public of the Government being transparent about their use of algorithms?

***Alexandra Sinclair:*** Thank you for the question. In order for the public to have trust and buy-in to these systems overall, so that they can benefit from them, they have to believe that their data is being used fairly and lawfully. That requires knowing which criteria are being used when making a decision, whether those criteria are relevant, and whether they are discriminatory or not. The first step to accountability is always transparency. You can know a decision is fair or lawful only if you know how the decision was made in the first place.

**Q153 Stephanie Peacock:** That is great. Could you tell us about your TAG transparency register and what it revealed about the level of transparency in Government algorithmic use?

***Alexandra Sinclair:*** Currently the Government have their algorithmic reporting transparency standard—I think I have got that right; they keep changing the acronym. Currently on that system there are about six reports of the use of automated decision-making technology in government. The Public Law Project decided to create a parallel register of the evidence that we could find for automated decision making in government. Our register includes over 40 systems in use right now that involve partly automated decisions about people. It would be great if the Government themselves were providing that information.

**Q154 Stephanie Peacock:** In the consultation, the Government said:

"There are clear benefits to organisations, individuals and society in explaining algorithmic decision-making"

in the public sector. Do you think that measures in the Bill achieve that? Do they unlock benefits and explain the Government's algorithmic decision making to the public?

***Alexandra Sinclair:*** No, and I think they do not do that for three reasons, if I have the time to get into this. The changes to subject access requests, to data protection impact assessments and to the prohibition on article 22 are the key issues that we see. The reason why we are particularly worried about subject access requests and data protection impact assessments is that they are the transparency provisions. They are how you find out information about what is happening. A subject access request is how you realise any other right in the Bill. You can only figure out if an error has been made about your data, or object to your data, if you know how your data is being used in the first place.

What we are worried about with the Bill is that you currently have an almost presumptive right to your data under a subject access request, but the change in the Bill changes the standard from the current "manifestly unfounded or excessive" to "vexatious or excessive". It also gives a whole load of factors that data controllers are now allowed to take into account when declining your request for your own data. Furthermore, under the proposal in the Bill they do not have to give you the reason why they declined your request for the data. We think that is really problematic for individuals. You have got this information asymmetry there, and it is going to be really difficult for you to prove that your request was not vexatious or excessive if you do not even know why it was denied in the first place.

If we think about some examples that we have been talking about in Committee today, in a lot of the Uber and Ola-led litigation, where individuals were able to show that their employment rights had been unfairly treated, they were able to find out about that through subject access requests. Another example is the London Met police's gangs matrix. The Information Commissioner's Office did a review of that matrix and found that the system did not even clearly distinguish between victims and perpetrators of crime, and the only way for individuals to access the matrix and check if the information held on them is accurate is through a subject access request. That is our first concern with the Bill.

Our second concern is the changes to data protection impact assessments. The first thing to note is that they already have to apply only in high-risk processing situations, so we do not think that they are an undue or onerous burden on data controllers because they are already confined in their scope. What a data protection impact assessment does—this is what we think is beneficial about it—is not to be a brake on processing, but to force data controllers to think though the consequences of processing operations. It asks data controllers to think, "Where is that data coming from? What is the data source? Where is that data being trained? For what purpose is that data being used?" The new proposal under the Bill for data protection impact assessments significantly waters down those obligations and means that, essentially, the only requirement is accounting for the purposes for the data. So instead of explaining how the data is being used, you are only requiring that purpose.

We think that has two problems. First, data controllers will not be thinking through all the harms and consequences before they deploy a system. Secondly, if individuals affected by those systems want to get information about how their data was processed and what happened, there will be a lot less information on that impact assessment for them to assess the lawfulness of that processing.

My final critique of the Bill is this. We would say that the UK is world-leading in terms of article 22—other states are certainly looking to the UK—and it is a

strange time to be looking to roll back protections. I do not know if Committee members have heard about how Australia recently experienced the Robodebt scandal, on which there is a royal commission at the moment. In that case, the system was a solely automated debt discrepancy system that ended up making over 500,000 incorrect decisions, telling people that they had committed benefit fraud when they had not. Australia is having to pay millions of dollars in compensation to those individuals and to deal with the human cost of that decision. The conversation in Australia right now is, "Maybe we should have article 22. Maybe this wouldn't have happened if we had had a prohibition on solely automated decision making." When other states are looking to beef up their AI protections, we need to think carefully about looking to roll them back.

**Q155 Stephanie Peacock:** Thank you for that really comprehensive answer.

Jacob, what measures do you think should be in place to ensure that data protection legislation balances the need to protect national security with the need to uphold human rights? Does the Bill strike the right balance?

***Jacob Smith:*** Thanks for the question. To take the second part first, we argue that the Bill does not strike the right balance between protecting national security and upholding data and privacy rights. We have three main concerns with how the Bill sets out that balance at the moment, and they come from clauses 24 to 26.

We have this altered regime of national security certificates for when law enforcement is taking measures in the name of national security, and we have this new regime of derogation notices. When law enforcement and the security services are collaborating, the notices allow the law enforcement body working in that collaboration to benefit from the more relaxed rules that are generally only for the intelligence services.

From our perspective, there are three main concerns. First, we are not quite sure why these amendments are necessary. Under human rights law, for an interference with somebody's data or privacy rights to be lawful, it needs to be necessary, and that is quite a high standard. It is not something akin to it being more convenient for us to have access to this data, or more efficient for us to have access to this data; it has to meet a high standard of strict necessity. Looking through the Second Reading debate, the impact assessment and the European convention on human rights analysis, there is no reference to anything that would be akin to necessity. It is all, "It would be easier for law enforcement to have these extra powers. It would be easier if law enforcement were potentially able to use people's personal data in more ways than they are at the moment." But that is not the necessity standard.

The second concern is the lack of safeguards in the Bill. Another thing that human rights law—particularly article 8 of the ECHR—focuses on is the necessity of introducing additional safeguards to prevent the misuse of legislation that allows public bodies to interfere with people's privacy rights. At the moment, as the Bill sets out, we have very weak safeguards when both national security certificates and designation notices are in place. At the moment, there is an opportunity, at least on the face of the Bill, for both those measures to be challenged before the courts. However, the issue here is that the Secretary of State has almost a monopoly over deciding whether those notices and certificates get published. So yes, although on the face of the Bill an individual may be able to challenge a national security certificate or a designation notice that has impacted them in some way, in practice they will not be able to do that if they do not know that it exists.

Finally, one encompassing issue is the expansive powers for the Secretary of State. One thing that we advocate is increased independent oversight. In the Bill, the Secretary of State has an extremely broad role in authorising law enforcement bodies to process personal data in a way that would otherwise be unlawful and go further than the existing regimes under the Data Protection Act 2018. Those are our three broad concerns in that regard. Ultimately, we do not see that the right balance has been made.

**Q156 Stephanie Peacock:** My final question is to all the witnesses. What are your views on the reforms to the ICO and their potential impact on its independence from Government?

***Ms Irvine:*** We have concerns about the proposed changes and their potential impact on the independence of the Information Commissioner. I was able to listen to John Edwards speaking this morning, and I noted that he did not share those concerns, which I find surprising. The ICO is tasked with producing statutory codes of conduct, which are incredibly useful for my clients and for anyone working in this sector. The fact that the Secretary of State can, in effect, overrule these is concerning, and it must be seen as a limit on the Information Commissioner's independence.

That leads to a concern that we have in relation to the adequacy decision that is in place between the EU and the United Kingdom. Article 52 of the GDPR states very clearly that a supervisory authority must have clear independence. The provisions relating to the independence of the Commission—the potential interference of the Secretary of State in law is enough to undermine independence—are therefore of concern to us.

***Alexandra Sinclair:*** We would just say that it is not typical for an independent regulator to have its strategic objectives set by a Minister, and for a Minister to set those priorities without necessarily consulting. We consider that the ICO, as subject matter experts, are probably best placed to do that.

***Jacob Smith:*** From our perspective, the only thing to add is that one way to improve the clauses on national security certificates and designation notices would be to give the ICO an increased role in oversight and monitoring, for instance. Obviously, if there are concerns about its independence, we would want to consider other mechanisms.

**Q157 Carol Monaghan** (Glasgow North West) (SNP): Laura Irvine, in your briefing about the Bill you raised concerns about some of the language. We had some discussion this morning about the language and particular terms, such as what "vexatious" means, for example. Could you elaborate on your concerns?

***Ms Irvine:*** Certainly. There are terms that have been used in data protection law since the 1984 Act. They were used again in the 1998 Act, echoed under the GDPR and included in all the guidance that has come from the Information Commissioner's Office over the past number of years. In addition to that, there is case law that has interpreted many of those terms. Some of

the proposed changes in the Bill introduce unexpected and unusual terms that will require interpretation. Even then, once we have guidance from the Information Commissioner, that guidance is sometimes not as helpful as interpretation by tribunals and courts, which is pretty sparse in this sector. The number of cases coming through the courts is limited—albeit that there is a lot more activity in the sector than there used to be. It simply presents a lot more questions and uncertainty in certain ways.

For my business clients, that is a great difficulty, and I certainly spend a lot of time advising clients on how I believe a matter—a phrase—will be interpreted, because I have knowledge of how data protection law works in general. That is based on my experience of the power of businesses and organisations, particularly in the third sector. Smaller bodies will often be challenged by a lack of knowledge and expertise, and that is a difficulty of introducing in legislation brand-new terms that are not familiar to practitioners, far less the organisations asked to implement the changes.

**Q158 Carol Monaghan:** You also raised concerns about automated decision making. Again, we have heard quite a lot about that today. You talked about a case on automated decision making, with regard to benefit awards being made by local authorities. Can you tell us a bit about that and where the danger might lie here?

***Ms Irvine:*** I expect that you have heard a lot of warnings about safety. I echo what Alexandra said earlier about the removal of the right not to have automated decisions taken by organisations. That is something that we were concerned to see in a society where this is happening more and more. The particular example that we gave came from a study that had been carried out by the Equality and Human Rights Commission. That was looking particularly at decision making in local authorities; at how AI or algorithms were being used to take decisions without enough transparency; and at whether this gave the individuals the right to challenge those decisions, which stems from the transparency that is built in. The challenge for any organisation using any automated decision making—particularly in the public sector, I would submit, where the impact can be extremely significant, particularly if we are talking about benefits—is making sure these organisations understand what the technology is doing, explaining that to individuals and giving them the right to object.

The changes in the Bill relax the restrictions on automated decision making and allow that to happen almost as a default, with safeguards as an add-on, whereas article 22 as currently drafted provides a right not to have automated decisions taken about an individual unless certain circumstances apply. To echo what Alexandra said, when more and more decisions are being made automatically without a human intervening, and certainly without a human intervening at the appropriate stage to prevent damage or harm to individuals, it would absolutely seem like the wrong time to make these changes and relaxations to the regime.

**Carol Monaghan:** Thank you.

**The Chair:** You have all been superstars in our 10th panel. Thank you very much indeed for the evidence you have given this afternoon. We will now move on to the next panel.

**Examination of Witness**

*Alex Lawrence-Archer gave evidence.*

4.17 pm

**The Chair:** We now come to our 11th and final panel. We are pleased to welcome Alex Lawrence-Archer, who is a solicitor for AWO. We have until 4.40 pm for this session. Alex, will you please introduce yourself to the Committee for the record?

***Alex Lawrence-Archer:*** Hi, I am Alex Lawrence-Archer. I am a solicitor and I litigate data rights cases at AWO. We were also instructed by Reset to help it to formulate its written evidence to the Committee, which hopefully you have received in the last couple of days.

**The Chair:** Thank you and welcome.

**Q159 Stephanie Peacock:** What are the main implications of the Bill for people's personal data rights?

***Alex Lawrence-Archer:*** There is a group of changes in the Bill that, perhaps in ways that were unintended or at least not fully thought through, quite seriously undermine the protection of individuals' privacy and data rights. A few of the most concerning ones are the change to the definition of personal data, recognising legitimate interests, purpose limitation, changes to the test for the exercise of data subject rights—I could go on. You will have heard about many of those today. It amounts to an undermining of data rights that seems not to be in proportion to the relatively modest gains in terms of reduction in bureaucracy on the part of data controllers.

**Q160 Stephanie Peacock:** Following on from that answer, what do you think the impact will be of the new definition of personal data as contained in the Bill?

***Alex Lawrence-Archer:*** It is quite difficult to predict, because it is complicated, but it is foundational to the regime of data protection. One of the issues is that in seeking to relieve data controllers of certain bureaucratic requirements, we are tinkering with these really foundational concepts such as lawful basis and the definition of personal data.

Two things could happen, I think. Some quite bad-faith arguments could be run to take quite a lot of processing outside the scope of the data protection regime. Although I doubt that those arguments would succeed, there is an additional issue; it is quite complicated to explain, but I will try. If it is unlikely but possible that an individual might be re-identified from a pseudonymised dataset—it could happen if there were a hack, say, but it is unlikely—that processing under the new regime would not, as the Bill is drafted, benefit from the protection of the regime. It would not be considered personal data, as it would not be likely that the individual could be identified from that dataset. That is a real problem because pseudonymised datasets are very common with large datasets. There are real risks there that would not be dealt with.

**Q161 Stephanie Peacock:** On average, how long does it currently take for data subjects to resolve basic data rights breaches?

***Alex Lawrence-Archer:*** Under the current regime, that is a bit like asking, "How long is a piece of string?" It can take quite a long time. There are certain practices

that the ICO follows in terms of requiring individuals to complain to the controller first. Some controllers are good; some are quick, but some are not. You might have a lot of back and forth about data access at the beginning, but other controllers might hand over your data really quickly. However, you could be looking at anything up to, say, 10 to 12 months.

**Q162 Stephanie Peacock:** Do you think that any changes in the Bill, for example those surrounding subject access requests, would increase that time?

***Alex Lawrence-Archer:*** Yes. You have heard from lots of people about the changes to the standard to be applied when any of the rights in chapter 3 are exercised by a data subject, and that includes the right of access. I think it is very likely that many more exercises of the right of access will be refused, at least initially. I think there will be many more complaints about the right of access and there is likely to be satellite litigation about those complaints as well, because you cannot proceed in finding out what has gone on with your data and rectify a problem unless you have access to the copies of it.

So, what you might find in many cases is a two-stage process whereby, first, you must resolve a complaint, maybe even a court case, about your right to access the data and then, and only then, can you figure out what has actually been going on with it and resolve the underlying unlawfulness in the processing. Effectively, therefore, it is a doubling of the process for the individual.

**Q163 Stephanie Peacock:** A final question: do you think that the definitions of "vexatious" and "excessive" are clear enough not to be abused by controllers who simply do not want to carry out subject access requests?

***Alex Lawrence-Archer:*** The new definitions, particularly the list of factors to be taken into consideration in determining whether the test is met, provide a lot of breathing room for controllers, whether or not they have good intentions, to make arguments that they do not need to comply with the right of access. If you are looking not to comply or if you have an incentive not to, as many controllers do, that does not necessarily mean that you are acting in bad faith; you might just not want to hand over the data and think that you are entitled not to do so. If you are looking not to comply, you will look at the Act and see lots of hooks that you can hang arguments on. Ultimately, that will come back to individuals who are just trying to exercise their rights and who will be engaged in big arguments with big companies and their lawyers.

**Q164 Damian Collins:** The age-appropriate design code for children was mentioned in our session this morning. Do you have any thoughts on what the Bill could mean for the application of that design code, which was obviously prepared for an environment in which GDPR was enshrined in UK data law?

***Alex Lawrence-Archer:*** The age-appropriate design code was a real success for the UK in terms of its regulation and its reputation internationally. It clarified the rights that children have in relation to the processing of their personal data. However, those rights are only helpful if you know what is happening to your personal data, and if and when you find out that you can exercise your rights in relation to that processing.

As I have said, what the Bill does—again, perhaps inadvertently—is undermine in a whole host of ways your ability to know what is happening with your personal data and to do something about it when you find out that things have gone wrong. It seems to me that on the back of a notable success in relation to the AADC, we are now, with this Bill, moving in rather a different direction in terms of that argument for protection of personal data.

Looking at the even longer term, there will be some slightly more nuanced changes if and when the AADC comes to be amended or redrafted, because of the role of the ICO and the factors that it has to take into account in its independence, which again you have already heard about. So you could, in the long term, see a new version of the AADC that is more business-friendly, potentially, because of this Bill.

**Q165 Damian Collins:** In terms of access to personal data, a lot of what we are talking about, certainly when we are talking about children, relates to what we generally call big-tech companies. A lot of the age-appropriate design code is focused on children's interface with services like Instagram, YouTube, TikTok and so on, of which they are heavy users. Are you concerned that because data may be stored in such a way that it is difficult for an external person to locate to an individual user, companies may use that as an excuse to be much looser in their application of the protections for children?

***Alex Lawrence-Archer:*** There are a bunch of different ways in which companies will take advantage of the new grey areas that the Bill opens up to carry out processing with less transparency and less respecting of the rights of the people whose data they are processing. If we take just the definition of research, for example, it will be much easier to carry out research for a large platform that already has lots of personal data. The GDPR already provides for a lot of exemptions when you are carrying out research; the Bill dramatically expands that definition. If you are a Google or a YouTube, then yes, you are much freer to carry out processing that you consider to be research without necessarily being transparent about it to the users affected, those whose data it concerns.

**Q166 Damian Collins:** The project that triggered the initial Cambridge Analytica scandal was in theory academic research on personality profiling, so there are lots of ways in which the definition can be stretched, for sure. Earlier, I asked the Information Commissioner about the definition of legitimate interests for companies. He seemed to think that if he thought that someone did not have a legitimate interest, he could still investigate it and therefore the Bill did not make much difference, but are you reassured by what he said?

***Alex Lawrence-Archer:*** We need to distinguish between two things: one is the introduction of some examples of what may be legitimate interests, which is not a particular concern because they replicate what is already in a recital; and, separately and of much greater concern, the introduction of recognised legitimate interests. I think that that is quite a radical departure from legitimate interests under the current regime. The Bill possibly misguides people, because it uses the language of legitimate interests, but it works in a very different way.

If you have a legitimate interest under the current regime, you must balance your interests against those of data subjects, and that is not something that is required if you can rely on a recognised legitimate interest under the new regime. The recognised legitimate interests are very broad—prevention of crime, for example, does not mean that that has to be done by the police. That is about opening up such processing for any kind of controller, which could be your neighbour or local corner shop, who can rely on that recognised legitimate interest with no requirement to consider the data subject's interest at all. That is a radical departure, because the concept of balancing the interests of the data subject and of the controller is absolutely fundamental to our current regime.

**Q167 Damian Collins:** In that case, on recognised legitimate interests, if someone says that their legitimate interest is the prevention of crime, they can define that in any way that they like in how they might seek to process or analyse behaviour patterns in their systems?

***Alex Lawrence-Archer:*** I do not want to overstate the case. You must be able to demonstrate that the processing is necessary for a recognised legitimate interest; it has got to make sense—but you do not have to consider anyone else's interests.

For example, in some recent cases, neighbours were operating CCTV that captured lots of the personal data of their neighbours. An important argument to show that that was unlawful was that yes, the processing was necessary for the detection of crime—that is what the CCTV was for—but the interests of the neighbours, views of whose gardens and front windows were being captured, overrode the legitimate interests of the controller. That is how it works under the current regime. Under the new regime, you would not have to consider the interests of the neighbours in the use of that CCTV system. You would be able to rely on the recognised legitimate interest.

**Q168 Damian Collins:** Effectively, you would not need to consider whether the use of that technology in that case was disproportionate to the risk.

***Alex Lawrence-Archer:*** Yes.

**Q169 Chi Onwurah:** We heard from some witnesses today that greater ease of access to data will increase competition for those such as Google and Meta that have large amounts of data as it is. What do you think the impact of this Bill will be for big tech?

***Alex Lawrence-Archer:*** I think the Bill is quite big tech-friendly, and the way that it deals with research is well illustrative of that. One of the objectives of the Bill is obviously to boost the use of personal data for academic research, which is a really laudable objective. However, the main change—in fact the only change I can think of off the top of my head—that it makes is to broaden the definition of academic research. That helps people who already have lots of personal data they might do research with; it does not help you if you do not have personal data. That is one of the major barriers for academics at the moment: they cannot get access to the data they need.

The Bill does nothing to incentivise or compel data controllers such as online platforms to actually share data and get it moving around the system for the purposes of academic research. This is in stark contrast to the approach being taken elsewhere. It is an issue the EU is starting to grapple with in a particular domain of research with article 40 of the Digital Services Act. There is a sense that we are falling behind a little bit on that key barrier to academic research with personal data.

**Q170 Chi Onwurah:** We also heard that existing cookie management and subject access requests and so on represent a real burden, particularly for smaller companies. Do you recognise that? Do you know why there is less support in technology to help small businesses deal with, if you like, the data management challenges? How is that to be traded off against the privacy rights of individuals?

***Alex Lawrence-Archer:*** I certainly recognise that the requirements of GDPR place compliance burdens on businesses of all sizes. I am sceptical that the right balance is being struck in trying to ameliorate the burdens of the costs and challenges that ordinary people will face—in terms of knowing how they are being profiled and tracked by companies—and resolving things when they have gone wrong. I am sceptical as well that there will be major benefits to many businesses who will continue to need to do business in Europe. For that reason, we will need either to have dual compliance or simply to continue to comply with EU GDPR. You can see this benefiting the largest companies, which can start to segment their users. We have already seen that with Meta, which moved its users on to US controllership, for example. I would see that as more beneficial to those large companies, which can navigate that, rather than, say, SMEs.

**The Chair:** Mr Lawrence-Archer, thank you very much for your time this afternoon.

That brings us to the end of our 11th panel. As an impartial participant in these proceedings—we have had over four-and-a-half hours of evidence with 23 witnesses—I would say it has been an absolute masterclass in all the most topical issues in data protection and digital information. Members might not realise it, but that is what we have had today.

*Ordered,* That further consideration be now adjourned. *—(Steve Double.)*

4.33 pm

*Adjourned till Tuesday 16 May at twenty-five minutes past Nine o'clock.*

## Written evidence reported to the House

DPDIB01 Judith Ratcliffe, Privacy Professional
DPDIB02 Dr C N M Pounder, Amberhawk Training Limited
DPDIB03 Prighter Ltd
DPDIB04 Damien Welfare
DPDIB05 Data and Marketing Association (DMA)
DPDIB06 Open Rights Group
DPDIB07 Big Brother Watch
DPDIB08 TrueLayer
DPDIB09 Internet Advertising Bureau (IAB) UK