PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT
GENERAL COMMITTEES

Public Bill Committee

DATA PROTECTION AND DIGITAL INFORMATION (NO. 2) BILL

First Sitting

Wednesday 10 May 2023

(Morning)

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

John Edwards, Information Commissioner, Information Commissioner's Office

Paul Arnold, ICO Deputy Chief Executive and Chief Operating Officer, Information Commissioner's Office

Eduardo Ustaran, Global co-head of the Hogan Lovells Privacy and Cybersecurity practice, Hogan Lovells

Vivienne Artz OBE

Bojana Bellamy, President, Centre for Information Policy Leadership

Neil Ross, Associate Director for Policy, TechUK

Chris Combemale, CEO, Data and Marketing Association

Dr Jeni Tennison OBE, Founder and Executive Director, Connected by Data

Anna Thomas, Co-Founder and Director, Institute for the Future of Work

Michael Birtwistle, Associate Director (AI Law and Regulation), Ada Lovelace Institute

Public Bill Committee

Wednesday 10 May 2023

(Morning)

[Mr Philip Hollobone *in the Chair*]

Data Protection and Digital Information (No. 2) Bill

9.25 am

The Chair: Before we begin, I have a couple of preliminary announcements that Mr Speaker has asked me to draw to your attention. *Hansard* colleagues would be grateful if Members emailed their speaking notes to hansardnotes@parliament.uk. Please switch electronic devices to silent. Tea and coffee are not allowed during sittings.

Today we will first consider the programme motion on the amendment paper. We will then consider a motion to enable the reporting of written evidence for publication and a motion to allow us to deliberate in private about our questions before the oral evidence session. In view of the time available, I hope we can take these matters formally—without debate. The programme motion was discussed yesterday by the Programming Sub-Committee for this Bill.

Ordered,

That—

1. the Committee shall (in addition to its first meeting at 9.25 am on Wednesday 10 May) meet—

(a) at 2.00 pm on Wednesday 10 May;

(b) at 9.25 am and 2.00 pm on Tuesday 16 May;

(c) at 11.30 am and 2.00 pm on Thursday 18 May;

(d) at 9.25 am and 2.00 pm on Tuesday 23 May;

(e) at 9.25 am and 2.00 pm on Tuesday 6 June;

(f) at 11.30 am and 2.00 pm on Thursday 8 June;

(g) at 9.25 am and 2.00 pm on Tuesday 13 June;

2. the Committee shall hear oral evidence in accordance with the following Table:

Date	Time	Witness
Wednesday 10 May	Until no later than 9.55 am	Information Commissioner's Office
Wednesday 10 May	Until no later than 10.25 am	Hogan Lovells; London Stock Exchange Group; Centre for Information Policy Leadership
Wednesday 10 May	Until no later than 10.50 am	techUK; Data & Marketing Association
Wednesday 10 May	Until no later than 11.25 am	Connected by Data; Institute for the Future of Work; Ada Lovelace Institute
Wednesday 10 May	Until no later than 2.25 pm	Medtronic; UK Biobank
Wednesday 10 May	Until no later than 2.50 pm	ZILO; UK Finance
Wednesday 10 May	Until no later than 3.05 pm	Better Hiring Institute
Wednesday 10 May	Until no later than 3.30 pm	National Crime Agency; Metropolitan Police
Wednesday 10 May	Until no later than 3.55 pm	Prospect; Trades Union Congress
Wednesday 10 May	Until no later than 4.25 pm	Public Law Project; Law Society of Scotland; Rights and Security International
Wednesday 10 May	Until no later than 4.40 pm	AWO

3. proceedings on consideration of the Bill in Committee shall be taken in the following order: Clauses 1 to 5; Schedule 1; Clause 6; Schedule 2; Clauses 7 to 11; Schedule 3; Clauses 12 to 20; Schedule 4; Clause 21; Schedules 5 to 7; Clauses 22 to 41; Schedule 8; Clauses 42 to 45; Schedule 9; Clauses 46 to 86; Schedule 10; Clauses 87 to 98; Schedule 11; Clause 99; Schedule 12; Clause 100; Schedule 13; Clauses 101 to 114; new Clauses; new Schedules; remaining proceedings on the Bill;

4. the proceedings shall (so far as not previously concluded) be brought to a conclusion at 5.00 pm on Tuesday 13 June.—*(Sir John Whittingdale.)*

Resolved,

That, subject to the discretion of the Chair, any written evidence received by the Committee shall be reported to the House for publication.—*(Sir John Whittingdale.)*

Resolved,

That, at this and any subsequent meeting at which oral evidence is to be heard, the Committee shall sit in private until the witnesses are admitted.—*(Sir John Whittingdale.)*

The Chair: Copies of written evidence that the Committee receives will be made available in the Committee Room and circulated to Committee members by email. We will now go into private session to discuss lines of questioning.

9.27 am

The Committee deliberated in private.

Examination of Witnesses

9.30 am

John Edwards and Paul Arnold gave evidence.

The Chair: We are now sitting in public again and the proceedings are being broadcast. Before we hear from the witnesses, do any Members wish to make a declaration of interest in connection with the Bill?

Jane Hunt (Loughborough) (Con): I am not sure whether this is a declaration of interest, so I will mention it just in case. I have had a meeting with Leicestershire Police Federation and I am interested in an amendment that it would like tabled.

Damian Collins (Folkestone and Hythe) (Con): I am not sure whether this is directly relevant to the Bill or adjacent to it, but I am an unpaid member of the board of the Centre for Countering Digital Hate, which does a lot of work looking at hate speech in the online world.

Mark Eastwood (Dewsbury) (Con): Given that one of today's witnesses is from Prospect, I wish to declare that I am a member of that union.

Stephanie Peacock (Barnsley East) (Lab): I am a proud member of a trade union. I refer the Committee to my entry in the Register of Members' Financial Interests.

Chi Onwurah (Newcastle upon Tyne Central) (Lab): I am a proud member of two trade unions.

Dr Rupa Huq (Ealing Central and Acton) (Lab): Should we declare our membership of any union?

The Chair: My advice is that it is always better to declare.

Dr Huq: Okay. I am a member of Unison, formerly the National and Local Government Officers Association.

Christian Wakeford (Bury South) (Lab): I am also a member of a union.

Mike Amesbury (Weaver Vale) (Lab): I am a member of Unison and the GMB.

The Chair: We will now hear oral evidence from John Edwards, the Information Commissioner, and Paul Arnold, the deputy chief executive and chief operating officer of the Information Commissioner's Office. I remind all Members that questions should be limited to matters within the scope of the Bill, and that we must stick to the timings in the programme order, which the Committee has agreed. For this panel, we have until 9.55 am. Will the witnesses please introduce themselves for the record?

John Edwards: Kia ora! My name is John Edwards. I am the Information Commissioner. I took up the job at the beginning of January last year. I was previously the Privacy Commissioner of New Zealand for eight years.

Paul Arnold: I am Paul Arnold, the deputy chief executive and chief operating officer of the ICO. I took up that position in 2016.

The Chair: May I gently say to the witnesses that this is a big room, so you will need to project your voices so that we can hear your evidence?

Q1 Stephanie Peacock: Good morning and welcome. The Bill creates a new body corporate to replace the corporation sole. What impact, both in the short and long term, do you think that will have on its ability to carry out its functions?

John Edwards: The corporation sole model is fit for a number of purposes. That was the structure that I had back home in New Zealand. For an organisation such as the Information Commissioner's Office, it is starting to buckle under the weight. It will benefit, I think, from the support of a formal board structure, with colleagues with different areas of expertise appointed to ensure that we bring an economy-wide perspective to our role, which as we have heard from the declarations of interest spans almost every aspect of human activity.

There will be some short-term, transitional challenges as we make the transition from a corporation sole to a board structure. We will need to employ a chief executive, for example, as well as getting used to those structures and setting up our new accountability frameworks. But I think, in the longer term, the model proposed in the legislation is well proven across other regulators, both domestically and internationally.

Q2 Stephanie Peacock: I would like to ask about the independence of the ICO as it stands. Do you have any experience of being directed by the Secretary of State in a way that has threatened the regulator's impartial position?

John Edwards: No, I do not.

Q3 Stephanie Peacock: If the Bill is passed in its current form, the Secretary of State—whoever that might be—will have the ability to approve and veto statutory codes of practice produced by the commission, as well as to set out a statement of strategic priorities to which the commission will have to adhere. Do you perceive that having any impact on your organisation's ability to act independently of political direction?

John Edwards: No, I do not believe it will undermine our independence at all. What I think it will do is to further enhance and promote our accountability, which is very important.

To take your first challenge, about codes of conduct, we worked closely with the Department for Digital, Culture, Media and Sport and subsequently the Department for Science, Innovation and Technology to ensure that we got the appropriate balance between the independence of the commission with the right of the Executive and Parliament to oversee what is essentially delegated lawmaking. I think we have got there. It is not a right to veto out of hand; there is a clear process of transparency, which would require the Secretary of State, in the event that he or she decided not to publish a statutory code that we had recommended, to publish their reasons, and those would be available to the House. I do think there is an appropriate level of parliamentary and Executive oversight of what is, as I say, essentially a lawmaking function on the part of the commission.

Q4 Stephanie Peacock: If the Secretary of State can veto a code of practice that the commission has produced regarding the activities of Government, will that not mean that they are, effectively, marking their own homework?

John Edwards: I do not believe so. The code of practice would be statutory—it is only the most serious statutory guidance that we would issue, not the day-to-day opinions that we have of the way in which the law operates. But, also, it is a reflection of the commissioner's view of the law, and a statement as to how he or she will interpret and apply the very general principles. A failure of the Secretary of State to table and issue a proposed code would not affect the way in which the commissioner

discharges his or her enforcement functions. We would still be able to investigate matters and find them in breach, regardless of whether that finding was consistent with the Secretary of State's view of the law.

Q5 Stephanie Peacock: I will come on to a slightly different topic now. The ICO will play a huge role in enforcing the measures in the Bill. Is there enough clarity in the Bill to ensure that the commission is able to do that effectively? For example, are you clear on how the commission will enforce the law surrounding terms like "vexatious" and "excessive" with regards to subject access requests?

John Edwards: Yes. We are in the business of statutory interpretation. We are given a law by Parliament. A term like "vexatious" has a considerable provenance and jurisprudence; it is one that I worked with back home in New Zealand. So, yes, I am quite confident that we will be able to apply those.

Q6 Stephanie Peacock: Linked to that, what about terms like "meaningful human involvement" and "significant decision" with regards to automated decision making?

John Edwards: Sorry, what is your question?

Stephanie Peacock: Parts of the Bill refer to there being "meaningful human involvement" and "significant decisions" within automated decision making. That might be in an application for a mortgage or in certain parts of employment. Do you feel that you can interpret those words effectively?

John Edwards: Yes, of course. You are quite right to point out that those phrases are capable of numerous different interpretations. It will be incumbent on my office to issue guidance to provide clarity. There are phrases in the legislation that Parliament could perhaps look at providing clearer criteria on to assist us in that process of issuing guidance—here I am particularly thinking of the phrase "high risk" activities. That is a new standard, which will dictate whether some of the measures apply.

Stephanie Peacock: That is useful. Thank you.

Q7 Damian Collins: Continuing with that theme, the Bill uses a broader definition of "recognised legitimate interests" for data controllers. How do you think the Bill will change the regime for businesses? What sort of things might they argue they should be able to do under the Bill that they cannot do now?

John Edwards: There is an argument that there is nothing under the Bill that they cannot do now, but it does respond to a perception that there is a lack of clarity and certainty about the scope of legitimate interests, and it is a legitimate activity of lawmakers to respond to such perceptions. The provision will allow doubt to be taken out of the economy in respect of aspects such as, "Is maintaining the security of my system a legitimate interest in using this data?" Uncertainty in law is very inefficient—it causes people to seek legal opinions and expend resources away from their primary activity—so the more uncertainty we can take out of the legislation, the greater the efficiency of the regulation. We have a role in that at the Information Commissioner's Office and you as lawmakers have just as important a role.

Q8 Damian Collins: How would you define that clarity that the Bill is seeking? If a data controller thinks, "Well, if I have legitimate business interests, I can make an excuse for doing whatever I like," that surely is not what the Bill intends. How would you define the clarity that you say the Bill seeks?

John Edwards: You are right that it is the controller's assessment and that they are entitled to make that assessment, but they need to be able to justify and be accountable for it. If we investigate a matter where a legitimate interest is asserted, we would be able to test that.

Q9 Damian Collins: How would you test it?

John Edwards: Well, through the normal process of investigation, in the same way as we do now. We would ask whether this was in the reasonable contemplation of the individual who has contributed their data as a necessary adjunct to the primary business activity that is being undertaken.

Q10 Damian Collins: Does this change things very much? It sounds like you are saying that business may assert it has a legitimate interest, but if you think it does not, you can investigate and take action as the law stands currently, effectively.

John Edwards: Yes, that is right. But the clarity will be where specific categories of legitimate interest are specified in the legislation. Again, that will just take out the doubt, if there is doubt as to whether a particular activity falls within scope.

Q11 Damian Collins: Is more clarity needed about the use of inferred data? Major social media platforms rely on inferred data to drive their recommendation tools and systems. There are then questions about whether inferred data draws on protected data characteristics without user permission. A platform might say that that is part of its recognised legitimate business interests, but users might say that it is an infringement of their data rights. Is that clear enough?

John Edwards: I am afraid that I have to revert to the standard, which is, "It depends." These are questions that need to be determined on a case-by-case basis after examination ex post. It is a very general question that you ask. It depends on what the inferred data is being used for and what it is. For example, my office has taken regulatory action against a company that inferred health status based on purchasing practices. We found that that was unlawful and a breach of the General Data Protection Regulation, and we issued a fine for the practice. Again, the law is capable of regulating inferred data, and there is no kind of carte blanche for controllers to make assumptions about people based on data points, whether collected from or supplied by the individual or not.

Q12 Damian Collins: Your predecessor raised the issue of the use of inferred data among users' protected data characteristics—political opinions, religious beliefs, sexual orientation—and said that, without the user's informed consent, that could not be legal. Do you agree with that?

John Edwards: I am not aware of the statement she made or the context in which she made it, so it is difficult for me to say whether she agreed it. Certainly,

informed consent is not the only lawful basis for a data processing activity and it may be that data about protected activities can be inferred and used in some circumstances. I would be happy to come back to you having checked that quote and to give you my views as to whether I agree with it in the context in which it was made.

Q13 Damian Collins: These are quite important matters because inferred data is such an important part of data processing for major platforms, be it a company assessing someone's attitude to risk and how that affects the way they might use a gambling product, versus taking someone's personal, private information, inferring things from it and making them open to suggestions they may not want to receive without their informed consent. That is a grey area, and I wonder whether you think the Bill provides greater clarity, or you think there needs to be more clarity still.

John Edwards: I think there is sufficient clarity. I am not sure whether the Bill speaks to the point you have just made, but for me the overarching obligation to use data fairly enables us to make assessments about the legitimacy of the kinds of practices you are describing.

The Chair: It is a really tight timetable this morning and we have nine minutes left. The Minister wants to ask some questions and there are three Members from the Opposition. I will call the Minister now. Perhaps you would be kind enough, Minister, to leave time for one question each from our three Members of the Opposition.

Q14 The Minister for Data and Digital Infrastructure (Sir John Whittingdale): Thank you, Mr Hollobone. Good morning, Mr Edwards. Both the structure and powers of your office are going to change as a result of the Bill. Do you believe that the existing structure and the absence of the powers you will gain under the Bill have in any way impeded the carrying out of your functions?

John Edwards: The obligation to investigate every complaint does consume quite a lot of our resources. Can I ask my colleague to make a contribution on this point?

Paul Arnold: As the commissioner says, that duty to investigate all complaints can challenge us in terms of where we need to dedicate the majority of our resources.

To the previous question and answer, our role in trying to provide or maximise regulatory certainty means being able to invest as much resource as we can in that upstream advice, particularly in those novel, complex, finely balanced, context-specific areas. We are adding far more value if we can add that support upstream.

The additional statutory objectives that are being added through the Bill overall will be a real asset to our accountability. Any regulator that welcomes independence also needs to welcome the accountability. It is the means through which we describe how we think, how we act and the outcomes that we achieve. Those extra statutory objectives will be a real aid to us and also an aid to Parliament and our stakeholders. It really does crystallise and clarify why we are here and how we will prioritise our efforts and resources.

Q15 Sir John Whittingdale: In the interests of time, I will ask you one other question. Mr Edwards, you had experience as the New Zealand Privacy Commissioner for some time. New Zealand is one of the countries recognised as having data adequacy by the European Union. Can you give us a view, based on your experience of dealing with the European Union, of whether there is any concern about the Bill that might put at risk the UK's data adequacy recognition from the EU?

John Edwards: I do not believe there is anything in the Bill that would put at risk the adequacy determination with the European Union. The test the Commission applies is whether the law is essentially equivalent. New Zealand lacks many of the features of the GDPR, as do Israel and Canada, each of which has maintained adequacy status. The importance of an independent regulator is preserved in this legislation. All the essential features of the UK GDPR or the rights that citizens of the European Union enjoy are present in the Bill, so I do not believe that there is a realistic prospect of the Commission reviewing negatively the adequacy determination.

The Chair: It is a brutal cut-off, I am afraid, at 9.55 am. I have no discretion in this matter. It is a quick-fire round now, gentlemen. We need quick questions and quick answers, with one each from Carol Monaghan, Chi Onwurah and Mike Amesbury.

Q16 Carol Monaghan (Glasgow North West) (SNP): Clause 40 sets out the criteria by which a data controller can refuse data access requests. Do you think this is appropriate? Are you concerned that it may lead to a situation in which only those who can afford to pay a potential fee will be able to access their data?

John Edwards: Yes and no. Yes, I do believe it is an adequate provision, and no, I do not believe there will be an economic barrier to people accessing their information rights.

Q17 Chi Onwurah: The Bill's intent is to reduce burdens on organisations while maintaining high data protection standards. Do you agree that high data protection standards are promoted by well-informed and empowered citizens? What steps do you think the Bill takes to ensure greater information empowerment for citizens?

John Edwards: Yes, I do believe that an empowered citizenry is best placed to enjoy these rights. However, I also believe that the complexity of the modern digital environment creates such an information asymmetry that it is important for strong advocates such as the Information Commissioner's Office to act as a proxy on behalf of citizenry. I do not believe that we should devolve responsibility to citizens purely to ensure that high standards are set and adhered to in digital industries.

Q18 Mike Amesbury: Drawing on your expertise, is there anything missing from the Bill that you would have liked to see?

John Edwards: I do not believe so. We have been involved right from the outset. We made a submission on the initial White Paper. We have worked closely with officials. We have said that we want to see the Bill get to a position where I, as Information Commissioner, am able to stand up and say, "I support this legislation." We have done that, which has meant we have achieved quite significant changes for the benefit of the people of the United Kingdom. It does not mean that we have just accepted what the Government have handed out. We

have worked closely together. We have acted as advocates, and I believe that the product before you shows the benefits of that.

The Chair: We have a late entry—the last question will be from Rupa Huq.

Q19 Dr Huq: When I was on the Criminal Finances Bill Committee, lots was promised, but the National Crime Agency then claimed that it was not financed enough to pursue all the unexplained wealth orders that were promised. Do you think that a beefed-up Information Commission will be sufficiently well resourced to do all the things it is meant to do?

John Edwards: In short, yes. We are having discussions about the funding model with DSIT. We are funded by levies. There are two questions: one is about how those levies are set and where the burden of funding our office lies in the economy, and the second is about the overall quantum. We can always do more with more. If you look at the White Paper on artificial intelligence and the Vallance report, you will see that there is a role for our office to patrol the new boundaries of AI. In order to do that, we will have to be funded appropriately, but I have a good relationship with our sponsor Department and am confident that we will be able to discharge all the responsibilities in the Bill.

The Chair: Gentlemen, thank you very much indeed for your evidence. You can now breathe, relax and enjoy the rest of your day.

Examination of Witnesses

Eduardo Ustaran, Vivienne Artz and Bojana Bellamy gave evidence.

9.53 am

Q20 The Chair: We will now hear oral evidence from Eduardo Ustaran, global co-head of the privacy and cyber-security practice at Hogan Lovells, who is appearing via Zoom; Vivienne Artz OBE, who is in the room; and Bojana Bellamy, president of the Centre for Information Policy Leadership, who is also appearing via Zoom. For this session we have until 10.25 am. Will the witnesses introduce themselves for the record, starting with Vivienne Artz?

Vivienne Artz: Good morning. My name is Vivienne Artz. I am the chair of the International Regulatory Strategy Group data committee, I have more than 25 years' experience in financial services, including acting as a chief privacy officer, and I now do advisory work across a range of sectors, including in the context of financial crime.

The Chair: Will Eduardo Ustaran please introduce himself? Can you hear us, Mr Ustaran? No. Can you hear us, Bojana Bellamy? No. Okay, we will start with our witness who has been kind enough to join us in the room.

Q21 Stephanie Peacock: Welcome. Vivienne, would you be in favour of implementing a smart data regime in your industry? If so, why?

Vivienne Artz: Yes, we are interested in implementing a smart data regime because it will allow broader access to data for innovation, particularly in the context of open banking and open finance. It would require access to information, which can often be limited at the moment. There is a lot of concern from businesses around whether or not they can actually access data. Some clarification on what that means, in respect of information that is not necessarily sensitive and can be used for the public good, would be most welcome. Currently, the provisions in the legislation are pretty broad, so it is difficult to see what it will look like, but in theory we are absolutely in favour.

Q22 Stephanie Peacock: Could you give more detail on who you think would benefit or lose out, and in what ways?

Vivienne Artz: Consumers would absolutely benefit, and that is where our priority needs to be—with individuals. It is an opportunity for them to leverage the opportunities that the data can provide. It will enable innovators to produce more products and services that will help individuals to better understand their financial and personal circumstances, particularly in the context of utility bills and so on. There are a number of positive use cases. There is obviously always the possibility that data can be misused, but I am a great advocate of saying that we need to find the positive use cases and allow business to support society and our consumers to the fullest extent. That is what we need to support.

Q23 Stephanie Peacock: Brilliant. What are your thoughts on giving the Secretary of State the power to amendment data protection legislation further? Do you think it is necessary to future-proof the Bill?

Vivienne Artz: It is necessary to future-proof the Bill. We are seeing such an incredible speed of innovation and change, particularly with regard to generative artificial intelligence. We need to make sure that the legislation remains technology-neutral and can keep up to date with the changes that are currently taking place.

Stephanie Peacock: I have more questions if our other witnesses are with us.

The Chair: We still have not heard definitively whether our other guests can hear us or speak to us, so we are waiting for confirmation from the tech people. In the meantime, I invite the Minister to question Vivienne Artz.

Q24 Sir John Whittingdale: You have a lot of experience in respect of international data transfers. The European Union has a number of data adequacy agreements around the world, but the process to establish them has been slow. How do you think the Bill will make it easier for us to improve international data agreements? What prospects are there for the UK to establish such agreements, and with which countries?

Vivienne Artz: The Bill provides for the opportunity for the Government to look at a range of issues and to move away from an equivalence approach to one in which we can consider more factors and features. The reality is that if you compare two pieces of legislation, you will always find differences because they come from different cultural backgrounds and different legal regimes. There will always be differences. The approach the UK is taking in the Bill is helpful because it looks at outcomes and broader issues such as the rule of law in different jurisdictions.

What is said on paper is not necessarily what always happens in practice; we need to look at it far more holistically. The legislation gives the Government the opportunity to take that broader and more common-sense view with regard to adequacy and not just do a word-by-word comparison of legislative provisions without actually looking at how the legislation is implemented in that jurisdiction and what other rights can support the outcomes. We can recognise that there is a different legal process and application but ask whether it still achieves the same end. That is what is really important. There is an opportunity not only to move more quickly in this space but to consider jurisdictions that might not be immediately obvious but none the less still offer appropriate safeguards for data.

Q25 Sir John Whittingdale: Obviously it is already possible for us to undertake international data transfers to countries with which we do not have an adequacy agreement. Can you set out the advantages of having a general adequacy agreement in terms of data transfer and the benefits to the UK economy?

Vivienne Artz: The current process is incredibly cumbersome for businesses and, if I am honest, it provides zero transparency for individuals as well. It tends to be mostly a paperwork exercise—forgive if that sounds provocative, but putting in place the model clauses is very often an expensive paperwork exercise. At the moment, it is difficult, time-consuming and costly, as the case may be.

The thing with adequacy is that it is achieved at a Government-to-Government level. It is across all sectors and provides certainty for organisations to move forward to share information, sell their goods and services elsewhere and receive those goods and services, and for consumers to access those opportunities as well. Adequacy is certainly the ideal. Whether it is achievable in all jurisdictions I do not know, but I think it is achievable for many jurisdictions to provide confidence for both consumers and businesses on how they can operate.

Sir John Whittingdale: Thank you.

The Chair: We can see Mr Ustaran and Ms Bellamy and they can hear us, but we cannot hear them, so we will carry on with questioning Vivienne Artz.

Q26 Carol Monaghan: A number of organisations have expressed concerns about moving to a situation in which we can refuse subject access requests or indeed charge a fee. Do you believe the thresholds in the Bill are appropriate and proportionate?

Vivienne Artz: I do think the thresholds are appropriate and proportionate. In practice, most organisations do not actually choose to charge, because actually it costs more to process the cheque than it is worth in terms of the revenue. Certainly, some sectors have been subject to very vexatious approaches through claims-management companies and others, where it is a bombarding exercise and it is unclear whether it is in the best interests of the consumers, or whether it is at their understanding and behest, to make a genuine subject access request.

I am a great supporter of subject access requests—they are a way for individuals to exercise their rights to understand what data is being processed—but as a result of quirks of how we operate often in the UK, they are being used as a pre-litigation investigative tool on the cheap, which is unfortunate and has meant that we have had to put in place additional safeguards to ensure they are used for the purpose for which they were provided, which is so that individuals can have transparency and clarity around what data is being processed and by whom.

Q27 Carol Monaghan: Do you think the threshold for something to be considered vexatious or excessive is well understood?

Vivienne Artz: We have heard from the Information Commissioner that they are fairly clear on what that terminology means and it will reflect the existing body of law in practice. I will be perfectly honest: it is not immediately clear to me, but there is certainly a boundary within which that could be determined, and that is something we would rely on the Information Commissioner to provide further guidance on. It is probably also likely to be contextual.

Q28 Carol Monaghan: How frequently do we expect such requests to be refused off the back of this legislation?

Vivienne Artz: I think it depends on the sector. I come from the financial services sector, so the types of subject access requests we get tend to be specific to us. I think organisations are going to be reluctant to refuse a subject access request because, at the end of the day, an individual can always escalate to the Information Commissioner if they feel they have been unfairly treated. I think organisations understand their responsibility to act in the best interests of the individual at all times.

Q29 The Chair: Ms Bellamy and Mr Ustaran, we can now hear both of you. Would you be kind enough to introduce yourselves?

Bojana Bellamy: Thank you for inviting me to this hearing. My name is Bojana Bellamy. I lead the Centre for Information Policy Leadership. We are a global data privacy and data policy think-and-do-tank operating out of London, Brussels and Washington, and I have been in the world of data privacy for almost 30 years.

Eduardo Ustaran: Good morning. My name is Eduardo Ustaran. I am a partner at Hogan Lovells, based in London, and I co-lead our global privacy and cyber-security practice, a team of over 100 lawyers who specialise in data protection law all over the world.

The Chair: Thank you. Chi Onwurah and Damian Collins are lined up to ask questions, but I want first to ask the shadow Minister whether she has any further questions, followed by the Minister. Because we have one witness in the room and two online, please will whoever is asking the question indicate whom you are asking it of?

Q30 Stephanie Peacock: Good morning to our guests joining us via Zoom. Ms Bellamy, in your opinion has it been difficult for businesses to adapt to the EU GDPR? If so, do you think the changes in the Bill will make it easier or harder for businesses to comply with data protection legislation?

Bojana Bellamy: Yes, certainly it has been hard to get businesses to comply with GDPR, in particular small and medium-sized businesses. I think the changes proposed in the Bill will make it easier, because it is more about

outcomes-based regulation. It is more about being effective on the ground, as opposed to being prescriptive. GDPR is quite prescriptive and detailed. It tells you how to do things. In this new world of digital, that is not very helpful, because technology always goes in front of and faster than the rules.

In effect, what we see proposed in the Bill is more flexibility and more onus on organisations in both the public and private sector to deliver accountability and effective protection for people. It does not tell them and prescribe how exactly to do that, yet they are still accountable for the outcomes. From that perspective, it is a step forward. It is a better regime, in my opinion.

Q31 Stephanie Peacock: Mr Ustaran, what do you perceive the value of EU adequacy to be? What would be the consequences for your businesses and other businesses and the UK market of losing such an agreement?

Eduardo Ustaran: From the point of view of adequacy, it is fundamental to acknowledge that data flows between the UK and the EU and the EU and the UK are essential for global commerce and for our digital existence. Adequacy is an extremely valuable element of the way in which the current data protection regime works across both the EU and the UK.

It is really important to note at the outset that the changes being proposed to the UK framework are extremely unlikely to affect that adequacy determination by the EU, in the same way that if the EU were to make the same changes to the EU GDPR, the UK would be very unlikely to change the adequacy determination of the EU. It is important to appreciate that these changes do not affect the essence of UK data protection law, and therefore the adequacy that is based on that essence would not be affected.

Q32 Stephanie Peacock: You have answered my next question—thank you—but I will pose it to the other witnesses, who may have something to add. In the previous session, the Information Commissioner said that he did not think the Bill was a threat to adequacy. That is comforting, but it is not confirmation, because the only people who have the power to decide whether adequacy stands are the European Commission. Do you think any of the measures in the Bill pose a risk to the adequacy agreement?

Bojana Bellamy: I certainly agree that adequacy is a political decision. In many ways—you have seen this with the Northern Ireland protocol—some of these decisions are made for different purposes. I do not believe there are elements of the Bill that would reduce adequacy; if anything, the Bill is very well balanced. Let me give you some examples of where I think the Bill goes beyond GDPR: certainly, on expectations of accountability on the senior responsible individual, which actually delivers better oversight and leadership over privacy; on the right to complain to an organisation and on organisations to respond to these complaints; and on the strong and effective Information Commissioner, who actually has more power. The regulator is smarter; that, again, is better than GDPR. There are also the safeguards that exist for scientific research and similar purposes, as well as some other detailed ones.

Yes, you will see, and you have seen in public projects as well, that there are people who are worried about the erosion of rights, but I do not believe that exception to subject access requests and other rights we talked about are actually a real erosion. I think it just clarifies what has been the law. Some of the requirements to simplify privacy impact assessment and records of processing will, in fact, deliver better accountability in practice. They are still there; they are just not as prescriptive. The Information Commissioner has strong powers; it is a robust regulator, and I do not believe its independence will be dented by this Bill. I say to those who think that we are reducing the level of protection that, actually, the balance of all the rules is going to be essential equivalency to the EU. That is really what is important.

May I say one more thing quickly? We have seen the EU make adequacy decisions regarding countries such as Japan and Korea, and even privacy shield. Even in these cases, you have not had a situation where the requirements were essentially equivalent. These laws are still different from GDPR—they do not have the right of portability or the concept of automated decision making—but they are still found to be adequate. That is why I really do not believe that this is a threat. One thing we have to keep absolutely clear and on par with the EU is Government access to data for national security and intelligence purposes. That is something the EU will be very interested in to ensure that that is not where the bar goes down, but there is no reason to believe so and there is nothing in the Bill to tell us so.

Vivienne Artz: I concur; I do not think the Bill poses any threat to adequacy with the EU. With regard to the national security issue that Bojana raises, I would also point out that the UN rapporteur noted that the UK has better protections for Government access to data than many EU member states, where it is often a very political approach as opposed to a practical approach and really looking at what the outcomes are. There is nothing in this Bill that would jeopardise adequacy with the EU.

The Chair: We have 12 minutes left and two Members are indicating that they wish to ask questions after you, Minister.

Q33 Sir John Whittingdale: I will be very quick, Mr Hollobone. Ms Bellamy, you have suggested that in some ways the regime that the Bill puts in place is superior to that of the existing GDPR and that it certainly does not risk our adequacy recognition in any way. Given the development of technology and the increasing use of things like AI, to what extent do you think the EU might follow the same sort of path that the Bill sets out to try to create a more flexible and a state-of-the-art regime?

Eduardo Ustaran: That is a very important question to address because perhaps one of the ways in which we should be looking at this legislative reform is a way of seeing how the existing GDPR framework that exists both in the EU and the UK could, in fact, be made more effective, relevant and modern to deal with the issues we are facing right now. You refer to artificial intelligence as one of those issues.

GDPR in the EU and the UK, is about five years old. It is not a very old piece of legislation, but a number of technological developments have happened in the past five years. More importantly, we have learned how GDPR operates in practice. This exercise in the UK is in fact very useful, not just for the UK but for the EU

and the world at large, because it is looking at how to reform elements of existing law that is already in operation in order to make it more effective. That does not mean that the law needs to be more onerous or more strict, but it can be more effective at the same time as being more pragmatic. This is an important optic in terms of how we look at legislative reform, and not only from the UK's point of view. The UK can make an effort to try to make the changes more visible outside the United Kingdom, and possibly influence the way in which EU GDPR evolves in the years to come.

Bojana Bellamy: I agree that we need a more flexible legal regime to enable the responsible use of AI and machine learning technologies. To be very frank with you, I was hoping the Bill would go a little further. I was hoping that there would be, for example, a recognition of the use of data in order to train algorithms to ensure that they are not discriminatory, not biased and function properly. I would have hoped that would be considered as an example of legitimate interests. That is certainly a way in which the Government can go further, because there are possibilities for the Secretary of State to augment those provisions.

We have seen that in the European AI Act, where they are now allowing greater use of data for algorithmic AI training, precisely in order to ensure that algorithms work properly. We have Dubai's data protection law and some others are starting to do that. I hope that we have good foundations to ensure further progression of the rules on AI. The rules on automated decision making are certainly better in this Bill than they are in GDPR. They are more realistic; they understand the fact that we going to be faced with AI and machine learning taking more and more decisions, of course with the possibility of human intervention.

Again, to those who criticise the rules, I would say it is more important to have these exposed rights of individuals. We should emphasise, in the way we have done in the Bill, the right to information that there is AI involved, the right to make a representation, the right to contest a decision, and the right to demand human review or human intervention. To me, that is really what empowers individuals and gives them trust that the decisions will be made in a better way. There is no point in prohibiting AI in the way GDPR sort of does. In GDPR, we are going to have something of a clash between the fact that the world is moving toward greater use of AI, and that in article 22 on automated decision making, there is a prohibition that makes it subject to consent or contract. That is really unrealistic. Again, we have chosen a better way.

As a third small detail, I find the rules on research purposes to be smarter. They are rather complicated to read, to be frank, but I look forward to the consolidated, clean version. The fact that technological development research is included in commercial research will enable the organisations that are developing AI to create the rules in a responsible way that creates the right outcomes for people, and does not create harms or risks. To me, that is what matters. That is more important, and that is what is going to be delivered here. We have the exemptions from notices for research and so on, so I feel we will have better conditions for the development of AI in a responsible and trusted way. However, we must not take our eyes off it. We really need to link GDPR with our AI strategy, and ensure that we incentivise organisations to be accountable and responsible when they are developing and deploying AI. That will be a part of the ICO's role as well.

The Chair: Five minutes left. This will be the quick-fire round. I have two Members indicating that they wish to ask questions—Chi Onwurah.

Q34 Chi Onwurah: Thank you, Mr Hollobone. We have heard that the intent in the Bill is in part to reduce the burden on organisations from data protection. We heard you set out what some of those burdens might be. The organisations affected by this Bill, and the organisations with which you work in different ways, operate in different jurisdictions. I think you, Ms Artz, set out quite well the challenges of having—or trying to have—the same regime in different jurisdictions. If forced to make a choice between following the European Union regime and following a divergent UK regime, what choice would the organisations with which you work make?

The Chair: Please choose one witness.

Chi Onwurah: Mr Ustaran, please.

Eduardo Ustaran: This is a question that many organisations that operate globally face right now. You must understand that data protection law operates all over the world and data flows all over the world, so consistency is really important in order to achieve compliance in an effective way. Therefore, a question—a very valid question—is, "Do I comply with the EU GDPR across the board, including in the UK, or should I make a difference?"

The reality is that when you look at the way in which the UK data protection framework is being amended, it provides a baseline for compliance with both the UK and EU regimes, in the sense that much of what is being introduced could potentially be interpreted as already being the case in the EU, if you apply perhaps a more progressive interpretation of EU law. Therefore, I think we should look just a little bit further than just saying, "Well, if I do comply with EU law, will I be all right in the UK?"

Maybe the way to look at it—something I see some organisations exploring—is, "If I were to take the UK interpretation of the GDPR on a wholesale basis, would that allow me to operate across the world, and certainly in the EU, in a more effective and efficient but still compliant way?" This is something that companies will be exploring, and it is not as easy as simply saying, "Well, I will just do EU law across the board."

Chi Onwurah: Could I—

The Chair: Sorry. It must be one quick question and one quick answer. We must finish at 10.25 am. Damian Collins.

Q35 Damian Collins: Ms Artz, one of the complaints about the current GDPR regime has been, for example, that oligarchs use it aggressively to target investigative journalists conducting legitimate investigations into their business activities, to bombard them with data access requests. Do you think that the provisions in the Bill around vexatious requests will help in that situation? Do you think that it will make any difference?

Vivienne Artz: I think it will help a little bit in terms of the threshold of "vexatious". I think the other piece that will help is the broadening of the provisions around legitimate interests, because now there is an explicit legitimate interest for fraud detection and prevention. At the moment, it is articulated mostly as to prevent a crime. I would suggest that it could be broadened in the context of financial crime, which has anti-money laundering, sanctions screening and related activities, so that firms can actually process data in that way.

Those are two different things: the one is processing data around sanctioned individuals and such like in the context of suspicious activities, and the other is the right of a subject access to remove their data. Even if they make that subject access request, the ability now to balance it against broader obligations where there is a legitimate interest is incredibly helpful.

The Chair: I thank all three witnesses for their time this morning and their extremely informative answers to the questions. Our apologies from Parliament for the tech issues that our two Zoom contestants had to endure. Thank you very much indeed. We will now move on to our third panel.

Examination of Witnesses

Neil Ross and Chris Combemale gave evidence.

10.25 am

Q36 The Chair: Welcome. We will now hear oral evidence from Neil Ross, Associate Director for Policy at techUK, and Chris Combemale—I hope I pronounced that correctly—the Chief Executive Officer of the Data and Marketing Association. Gentlemen, this session, as you have seen from the previous two, has to end no later than 10.50 am. I will be grateful if you could be kind enough, please, to introduce yourselves to the Committee for the record.

Neil Ross: Thank you for having us before the Committee. My name is Neil Ross. I am the Associate Director for Policy at techUK, the trade association that represents the technology sector in the UK. We have 950 companies in our membership.

Chris Combemale: I am Chris Combemale, the CEO of the Data and Marketing Association. I have 40 years' experience as a practitioner in marketing and advertising. I started on the agency side, including well-known brands, leading marketing technology business and first-generation cloud marketing technology.

The Chair: I apologise for getting your surname pronunciation wrong, Mr Combemale.

Chris Combemale: That's okay, it happens all the time. It is actually of French heritage, rather than Italian.

Q37 Stephanie Peacock: Welcome to the witnesses. TechUK's response to the withdrawn Bill last autumn stated that it

"could go further in seeking the full benefits of data driven innovation".

Does this amended Bill go further?

Neil Ross: Yes, it does. If we go back to the statement of the Information Commissioner earlier, the most important part of the legislation is to provide increased clarity on how we can use data. I think there were about 3,000 responses to the consultation, and the vast majority—particularly around the scientific research and the legitimate interest provisions—focused on providing that extra level of clarity. What the Government have done is quite clever, in that they have lifted examples from the recitals—recital 157, as well as those related to legitimate interests—to give additional clarity on the face of the Bill, so that we can take a much more innovative approach to data management and use in the UK, while still maintaining that within the broad umbrella of what means we qualify for EU adequacy.

Q38 Stephanie Peacock: How have your members found adapting to GDPR? Will the Bill make it easier or harder for those that you represent to comply?

Neil Ross: Most tech companies have adapted to GDPR. It is now a common global standard. The Bill makes the compliance burden a little easier to use, allows us to be a little more flexible in interpretation of it and will give companies much more certainty when taking decisions about data use.

One really good example is fraud. Online fraud is a massive problem in the UK and the Government have a strategy to deal with it, so having that legitimate interest that focuses on crime prevention—also those further processing rights around compliance with the law—means that we can be much more innovative and adaptive about how we share and process data to protect against and prevent fraud. That will be absolutely vital in addressing the shared objective that we all have to reduce online fraud.

Q39 Stephanie Peacock: On the changes to requirements to report suspicious activity related to unsolicited direct marketing, do the telecoms companies among your members have the technical capability to identify instances of mass unsolicited direct marketing in order to report as required?

Neil Ross: No. That is one area where we think further work is needed in the Bill. I think you are referring to clause 85. When we responded to the consultation, we said that the Government should try to create equivalence between the private communications requirements and the GDPR to give that extra level of flex. By not doing that and by not setting out specific cases of where telecoms companies have to identify unsolicited calls, the Government are being really unfair in what they are asking them to do. We have had concerns raised by a range of companies, both large and small, that they might not have the technical capability and that they will have to set up new systems to do it. Overall, we think that the Bill makes a bit of a misstep here and that we need to clarify exactly how it will work. TechUK and some of my colleagues will be suggesting to the Committee some legal amendments for how to do that.

Q40 Stephanie Peacock: On that point, do the telecoms companies feel that they have been consulted properly in the making of the legislation?

Neil Ross: No, not on that clause, but yes in relation to the rest of the legislation.

Q41 Stephanie Peacock: I was asking about that. Chris, will the changes to the cookies set out in the Bill benefit, first, the consumer experience and, secondly, your members or businesses?

Chris Combemale: Yes. First, on the consumer experience, I think that we all recognise that the pop-up consent banners for cookies are generally ticked as a matter of course by consumers who really want to go about their business and get to the website that they want to do business on. In a way, it is not genuine consent, because people are not really thinking deeply about it.

In terms of business, a number of the cookies, which are really identifiers that help you understand what people are doing on your website, are used just on a first-party basis by websites, such as e-commerce websites and business-to-business websites, to understand the basic operational aspects and statistical measurement of how many people are going to which pages. Those are websites that do not take any advertising and do not share any data with third parties, so the exemptions in the Bill generally would make those types of companies no longer need cookie banners while providing no risk to the customers, because the company uses the cookies purely to understand the behaviours of its own website traffic and its own customers. In that sense, we strongly support the provisions and the exemptions in the Bill.

Q42 Stephanie Peacock: Is the technology available to centralise cookies by browser?

Chris Combemale: I think it can be eventually, but we oppose those provisions in the Bill, because they create a market imbalance and give control as a gateway to large companies that manage browser technology, at the expense of media owners and publishers that are paying journalists and investing in content. It is incumbent upon all else that media owners are able to develop first-party relationships with their audiences and customers to better understand what they need. If anything, we need more control in the hands of the people who invest in creating the content and in paying the journalists who provide those important democratic functions.

Q43 Stephanie Peacock: Is there a concern that centralising cookies by browser will entrench power in the hands of the larger tech companies that own the browsers?

Chris Combemale: It certainly would give even greater market control to those companies.

Q44 Stephanie Peacock: Is the risk in centralising cookies by browser that we could confuse liability, for example who is responsible for a breach of cookie regulation?

Chris Combemale: I think it could be. For us, the essential principle is that a business, whether a media owner, e-commerce business or publishing business, should have control of the relationships between its products and services and its customers and prospects for its customers. By nature, when you give control to a third party, whether a large tech company or another company, you are getting in between the relationship between people and the organisations that they want to do business with and giving control to an intermediary who may not understand. At the least point, if you register with a website after, for instance, changing your browser setting, that should take precedence over the browser setting: your choice to engage with a particular company should always take precedence over a centralised cookie management system.

Neil Ross: I think that what the Government have done in relation to this is quite clever: they have said that their objective is to have a centralised system in the future, but they have recognised that there are a number of different ongoing legislative and regulatory activities that have a significant bearing on that. I think it was only last week that the Government introduced the Digital Markets, Competition and Consumers Bill, clause 20 of which—on conduct requirements—would play a large role in whether you could set up a centralised system, so there is an element of co-ordinating two different but ongoing regulatory regimes. I think we agree with Chris that the steps on analytical cookies now are good but that we need to have a lot more deep thought about what a centralised system may or may not look like and whether we want to go ahead with it.

Chris Combemale: May I come in on that final point? What makes sense to us is a centralised system for managing opt-outs as opposed to managing consent. As the Data and Marketing Association, we operate the telephone preference service and the mailing preference service, which give consumers the opportunity to opt out from receiving unwanted cold calls or unwanted direct mail. There is already a system in place with digital advertising—an icon that people can use to opt out from the use of personal data for personalising digital ads. I think it makes sense that, if people do not want to receive certain things, they can opt out centrally, but a centralised consent opt-in gives too much control to the intermediaries.

Stephanie Peacock: Thank you.

Q45 Sir John Whittingdale: Mr Ross, I know that techUK has been supportive of a number of elements of the Bill, particularly around the opportunities created by the use of smart data. Will you set out your view of the opportunities, and how the Bill will help to attain them?

Neil Ross: Smart data is potentially a very powerful tool for increasing consumer choice, lowering prices and giving people access to a much broader range of services. The smart data provisions that the Government have introduced, as well as the Smart Data Council that they are leading, are really welcome. However, we need to go one step further and start to give people and industries clarity around where the Government will look first, in terms of what kind of smart data provisions they might look at and what kind of sectors they might go into. Ultimately, we need to make sure that businesses are well consulted and that there is a strong cost-benefit analysis. We then need to move ahead with the key sectors that we want to push forward on. Similarly to on nuisance calls, we will send some suggested text to the Committee to add those bits in, but it is a really welcome step forward.

Q46 Sir John Whittingdale: Which particular sectors offer the most opportunity?

Neil Ross: I do not want to name specific sectors at this point. We are having a lot of engagement with our members about where we would like to see it first. The transport sector is one area where it has been used in the past and could have a large use in the future, but it is something that we are exploring. We are working directly

with the Government through the Smart Data Council to try to identify the initial sectors that we could look at.

Q47 Sir John Whittingdale: Thank you. Mr Combemale, will you set out some of the obstacles for your organisation, and how you would like the Bill to reduce them?

Chris Combemale: I think the single biggest one that has troubled our members since the implementation of GDPR is the issue around legitimate interest, which was raised by the hon. Member for Folkestone and Hythe. The main issue is that GDPR contains six bases of data processing, which in law are equal. For the data and marketing industry, the primary bases are legitimate interest and consent. For some reason it has become widely accepted through the implementation of GDPR that GDPR requires consent for marketing and for community activities. I am sure that you hear in your constituencies of many community groups that feel that they cannot go about organising local events because they must have consent to communicate. That has never been the intention behind the legislation; in fact, the European Court of Justice has always ruled that any legal interest could be a legitimate interest, including advertising and marketing.

If you look at what we do, which is effectively finding and retaining customers, the GDPR legislation says in recital 4 that privacy is a fundamental right, not an absolute right, and must be balanced against other rights, such as the right to conduct a business. You cannot conduct a business without the right to find and retain customers, just as you cannot run a charity without the right to find donors and volunteers who provide the money and the labour for your good cause. The clarification is really important across a wide range of use cases in the economy, but particularly ours. It was recognised in GDPR in recital 47. What the legislation does is give illustrative examples that are drawn from recitals 47, 48 and 49. They are not new examples; they are just given main text credibility. It is an illustrative list. Really, any legal interest could be a legitimate interest for the purpose of data providing, subject to necessity and proportionality, which we discussed earlier with the Information Commissioner.

Q48 Carol Monaghan: We have heard already this morning that a number of words and phrases could have some ambiguity associated with them, such as the word "excessive", and the Bill allowing certain cookies that are "low risk". Do you think that the phrase "low risk" is well enough understood?

Chris Combemale: In the sector that I represent, we have a fairly clear understanding of the gradients of risk. As I was saying earlier, many companies do not share data with other companies. They are interested solely in the relationships that they have with their existing customers or prospects. In that sense, all the customer attitudes to privacy research that we do indicates that people are generally comfortable sharing data with companies they trust and do business with regularly.

Q49 Carol Monaghan: Would that then be the definition of low risk?

Chris Combemale: I would not want to suggest what the legal definition is. To us in direct marketing and in the Data and Marketing Association, existing customer relationships—loyal customers who trust and are sometimes passionate about the brands they interact with—are low risk. Higher risk is when you come to share data with other companies, but again much of that activity and data sharing is essential to creating relevance. With the right protections, it is not a hugely high-risk activity. Then you can move on up, so the higher the degree of automation and the higher the degree of third-party data, the greater the risk, and you have to put in place mitigations accordingly. I am not a lawyer—I am just a poor practitioner—so I cannot define it from a legal point of view, but it is clear in the context of our industry how risk elevates depending on what you are doing.

Q50 Carol Monaghan: I might come back to that in a second, but I think Neil wanted to add something.

Neil Ross: I was going to say that you can see how Chris has interpreted it through the lens of his industry, but the feedback we have had from our members, who operate across a range of industries, suggests that there is quite a lot of confusion about what that terminology might mean. The rest of the Bill aims to clarify elements of the GDPR and put them on the face of the Bill, but this provision seems to be going in the other direction. It raises concern and confusion.

That is why our approach has always been that you are going to get more clarity by aligning the Privacy and Electronic Communications Regulation 2003 more with the GDPR, which has clear legal bases, processes and an understanding of what is high and low risk—a balancing test, and so on—than through this fairly broad and poorly understood term "low risk". We have concerns about how it will operate across a range of sectors.

Q51 Carol Monaghan: Chris, you said that you are not a lawyer and cannot define what low risk is, but there will of course have to be some sort of definition. Have we captured that well enough?

Chris Combemale: Coming back to our discussion about legitimate interest and the proportionality balancing test, or legitimate interest impact assessments, when you are thinking about what you are planning to do with your customers, it is a requirement of good marketing without the legislation, but also within the legislation, to think about how what you are planning to do will impact your customers' privacy, and then to mitigate. The important thing is not to say, "There's no risk," "It is low risk," or "It is high risk"; it is to understand that the higher the risk, the greater the mitigations that you have to put in place. You may conclude that you should not do something because the risk level is too high. That is what balancing tests do, and decisions and outcomes result from them.

Q52 Carol Monaghan: The potential difficulty here is that the responsibility is being put on the company. You have described a responsible company that categorises levels of risk and takes action accordingly. Without a clear definition, if it were a less scrupulous company, would there be a grey area?

Chris Combemale: We do a lot of work combating rogue traders, and we provide evidence to cases from our work with the telephone preference service and

other activities. Rogue traders—especially those with criminal intent—will generally ignore the legislation anyway regardless of what you do and whether it lacks clarity or not, but I think you are right. An important part of GDPR is that it puts a lot of responsibility on companies to consider their particular activity, their particular customer base and the nature of their audience. Age UK, a charity that has a lot of vulnerable elderly customers, has to have greater protections and put more thought into how it is doing things than a nightclub marketing to under-30s, who are very technologically literate and digitally conversant.

When we do customer attitudes to privacy studies, we see three broad segmentations—data unconcerned, data pragmatist and data fundamentalist—and they require different treatment. It is incumbent on any company, in a marketing context, to understand who their audience and their customer base is, and design programmes appropriately to build trust and long-term relationships over time. That is an important element of GDPR, from a marketer's perspective. I should add that it should not take legislation to force marketers to do that.

The Chair: There are five minutes left and there are two Members seeking to ask questions.

Q53 Damian Collins: With regards to children's data rights, do you think the Bill will have any implications for the way in which the age-appropriate design code has been implemented by companies working within it at the moment? It is not expressly written into the Bill, but do you expect there to be change?

Neil Ross: No, I do not expect so. Given some of the exemptions for further processing, it might help improve compliance with the law, because compliance with the law in the public interest is then a basis on which you could process data further. It might make it easier for companies to implement the age-appropriate design code.

Q54 Damian Collins: Can you give any examples of that?

Neil Ross: It just gives additional clarity on when and where you can use data on various grounds. There are a wide range of circumstances that you can run into in implementing the age-appropriate design code, so having more flexibility in the law to know that you can process data to meet a legal objective, or for a public interest, would be helpful. The best example I can give is from the pandemic: the Government were requesting data from telecoms companies and others, and those companies were unsure of the legal basis for sharing that data and processing it further in compliance with a Government or regulator request. The Bill takes significant steps to try and improve that process.

Q55 Damian Collins: Could you give an example more directly related to children?

Neil Ross: I do not have one to hand, but we could certainly follow up.

Q56 Mike Amesbury: The Bill enables the commissioner to impose a fine of £1,000. Is that a reasonable deterrent?

Neil Ross: That is in relation to clause 85?

Q57 Mike Amesbury: For non-compliance.

Neil Ross: We do not think it is particularly appropriate for this scenario, given that the telecoms operators are just informing the ICO about activity that is happening on their service. It is not that they are the bad actors in the first instance; they are having to manage it. Ultimately, the first step is to clarify the aims of clause 85, and then whether the fine is appropriate is a subsequent question.

Q58 Mike Amesbury: For some companies, £1,000 will be small fry.

Neil Ross: It will vary from company to company. Most companies will always seek to comply with the law. If you feel you need some kind of deterrent, that is something for Parliament to consider. The first step is to make sure that the law is really clear about what companies are being asked to do. At the moment, that is not the situation we are in.

The Chair: There are two minutes left. Chi Onwurah has the last question.

Q59 Chi Onwurah: Mr Combemale, you set out some of the challenges of having centralised cookie management, and how that would give more power to the browsers. What you did not set out was how we could give more control and power to customers—citizens—over how they use their data. What are you doing to ensure that consumers have more control over how their data is used? You talked about the little thing that you can click to stop our personal data being used—that has been in place for some time now and it is great. If we have the time, Mr Ross, what is your sector doing as well, because the technology should be there to help and empower people?

Chris Combemale: I think a lot of what our sector does voluntarily—setting aside the legislation—is the creation of what are called permission centres. You will be familiar with them from when you go to a website and it asks about categories of information or products that you are interested in. That allows consumers to express their interest. Within the legislation there is very clear data notification, required at the point that data is collected, which requires companies to ask you what you want to do. Whether it is consent or legitimate interest, consumers always have the right to opt out.

With marketing, there is an absolute right to ask not to receive marketing of any kind, whether that is email, direct mail or telephone, at any time. Companies have an obligation to follow that. When it comes to marketing, which is my subject matter expertise, consumers are very well protected and do exercise their rights to opt out. They are further protected by central services, for example the telephone preference service. That is a law that companies can look up; 70% or so of households have registered their telephone number there. I think there are a large number of protections in place, both through the legislation and voluntarily.

Q60 The Chair: Mr Ross, you have 30 seconds.

Neil Ross: There has been a big drive among many tech companies to explain better how they use and handle data practices. There is a drive within the sector to do that anyway. Some of that has come from legislative regulatory activity—for example, the Online Safety Bill and other places.

One thing I would say about this legislation is that it does give people more control over data through the privacy management frameworks. By taking a less strict tick-box approach to data-handling practices, there is the opportunity for core sectors or interest groups such as trade unions to put forward what their ideal data-handling practice should be for a company. As long as that complies with what the ICO sets out or the broad guardrails, then you can see a range of different handling practices adopted, depending on which sector you are in. That flexibility gives some power back to consumers and other interest groups.

The Chair: Gentlemen, you have been brilliant. Thank you very much indeed for your time this morning. We will now move on to the fourth panel.

Examination of Witnesses

10.50 am

Dr Jeni Tennison, Anna Thomas and Michael Birtwistle gave evidence.

Q61 The Chair: We will now hear oral evidence from Dr Jeni Tennison, founder and executive director of Connected by Data; Anna Thomas, co-founder and director at the Institute for the Future of Work; and Michael Birtwistle, associate director of AI law and regulation at the Ada Lovelace Institute. For this session we have until 11.25 am. Will the witnesses, from right to left, please be kind enough to introduce themselves to the Committee for the record?

Dr Tennison: Thank you very much for inviting me here today. My name is Dr Jeni Tennison. I am the executive director of Connected by Data, which is a campaign to give communities a powerful say in decisions about data. Prior to that I was the CEO of the Open Data Institute. I am also the co-chair of the data governance working group in the Global Partnership on Artificial Intelligence.

Anna Thomas: Good morning and thank you for having me. I am Anna Thomas, a founding director of the Institute for the Future of Work, a research and development institute exploring the impact of new technologies on work and working lives. I was formerly an employment barrister at Devereux Chambers. The institute is also the strategic research partner for the all-party parliamentary group on the future of work.

Michael Birtwistle: Good morning. I am Michael Birtwistle, an associate director at the Ada Lovelace Institute, responsible for law and policy. The Ada Lovelace Institute is an independent research institute with a mission to make sure that data and AI work for people and society. I was previously a policy adviser at the Centre for Data Ethics and Innovation.

The Chair: Welcome. Stephanie Peacock will start the questions.

Q62 Stephanie Peacock: Good morning. To go first to Dr Jeni Tennison, do you think the general public and workers have a good level of trust and understanding in terms of how their data is being used? What does the Bill do, if anything, to help build or improve on that trust and understanding?

Dr Tennison: Surveys and public attitudes polling show that when you ask people about their opinions around the use of data, they have a good understanding about the ways in which it is going wrong, and they have a good understanding about the kinds of protections that they would like to see. The levels of trust are not really there.

A poll from the Open Data Institute, for example, shows that only 30% trust the Government to use data ethically. CDEI has described this as "tenuous trust" and highlighted that about 70% of the public think that the tech sector is insufficiently regulated. I do not think that the Bill addresses those issues of trust very well; in fact, it reduces the power individuals have and also the level of collective representation people can have, particularly in the work context. I think this will diminish trust in the way in which data is used.

Q63 Stephanie Peacock: Do you believe the Government have consulted the public and data subjects such as workers appropriately during the process of formulating the Bill?

Dr Tennison: Obviously, there was a strong consultation exercise around the data reform Bill, as it was then characterised. However, there are elements of this Bill, in particular the recognised legitimate interests that are listed, that have not had detailed public consultation or scrutiny. There are also not the kinds of provisions that we would like to see on ongoing consultation with the public on specific questions around data processing in the future.

Q64 Stephanie Peacock: What value do subject access requests hold for citizens, and how will changing the threshold for refusing a request or changing a request to "vexatious or excessive" impact citizens' ability to exercise their rights?

Dr Tennison: Subject access requests are an important way in which citizens can work out what is happening within organisations with the data that is being held about them. There are already protections under UK GDPR against vexatious or excessive requests, and strengthening those as the Bill is doing is, I think, going to put off more citizens from making these kinds of requests.

It is worth noting that this is a specific design of the Bill. If you look at the impact assessment, this is where most of the cost to business is being saved; that is being done by refusing subject access requests. So I think we should be suspicious about what that looks like. Where we have been looking at the role of subject access requests in people exercising their rights, it is clear that that is a necessary step, and delays to or refusals of subject access requests would prevent people from exercising their rights.

We think that a better way of reducing subject access requests would be to have publication of things like the risk assessments that organisations have to do when there is high-risk processing—so that there is less suspicion on the part of data subjects and they do not make those requests in the first place.

Q65 Stephanie Peacock: Thank you. I have a couple of questions for Anna Thomas now. Do the current laws around automated decision making do enough to protect workers and citizens from harm?

Anna Thomas: Referring partly to our work in "Mind the gap" and "The Amazonian Era", as well as the report by the all-party parliamentary group on the

future of work about use of AI in the workplace, we would say no. The aim of the Bill—to simplify—is very good. But particular areas in the Bill as it stands—eroded somewhat—are particularly problematic in the workplace. The automated ones that you ask about are really important with regard to the reduction of human involvement. But in addition to that are the need to assess in advance what the risks and impacts are, the requirement for consultation, and the access to relevant information. Those are all relevant and overlap with the automated decision making requirement.

Q66 Stephanie Peacock: Linked to that, do you believe that the safeguards outlined in the Bill—having a right to human review, for example—are enough to protect workers from the potential harm of automated decision making?

Anna Thomas: Not in themselves. There is potential, in those areas, to correct that or to improve it in the course of the Bill's proceedings, in order that the opportunities, as well as the risks, of putting this new Bill through Parliament are seized. But, no, because of the transformation of work and the extent of the impact, as well as the risks, that new technologies and automated technologies are having across work, not just on access to work, but on terms, conditions, nature, quality and models for work, the safeguards—there is, I think, increasing cross-party consensus about this—should be, in those areas, moving in the other direction.

Q67 Stephanie Peacock: My final question is to Michael. Do you believe that the current regulation does enough to govern the use of biometric technologies?

Michael Birtwistle: No, we would say that it does not. The Ada Lovelace Institute published a couple of reports last year on the use of biometric data, arguing for a much stronger and coherent regulatory governance framework for biometric technologies. These are a set of technologies that are incredibly personal. We are used to their being talked about in terms of our faces or fingerprints, but actually it is a much wider range, involving any measurement to do with the human body, which can be used in emotional analysis—walking style or gait, your tone of voice or even your typing style. There is also a set of incoming, next-generation AI technologies that rely quite heavily on biometrics, so there is a question about future-proofing the Bill.

We have made two broad proposals. One is to increase the capability of the Information Commissioner's Office to look specifically at biometrics—for example, to create and maintain a public register of private entities engaging in processing of biometric data, to have a proper complaints procedure, to publish annual reports and so on. There is a set of issues around increasing the capability of our institutions to deal with that.

Then there is a second question about scope. First, the current focus of biometric data and definition is on identifiability of personal data. There are many potentially problematic use cases of biometric data that do not need to know who you are in order to make a decision about you. We think it would be wise and would future-proof the regulation of this powerful technology to also include classification or categorisation as the purpose of those biometric technologies.

Q68 Damian Collins: You make a very interesting point there, Mr Birtwistle. With automated decision making, a lot of that could be done anonymously. The user is just the end product. They are being targeted through systems and do not need to be identified; the systems just need to know what their data profile is like in order to make a decision.

I am interested in the views of the other members of the panel as well. Do you think there needs to be a greater onus on data controllers to make clear to regulators what data they are gathering, how they are processing it and what decisions are being made based on that data, so that, particularly in an automated environment, while there may not be a human looking at every step in the chain, ultimately a human has designed the system and is responsible for how that system is working?

Michael Birtwistle: I think that is a really important point that is going to be very relevant as we read this Bill alongside the AI White Paper provisions that have been provided. Yes, there is definitely a need for transparency towards regulators, but if we are thinking about automated decision making, you also want a lot of the safeguards and the thinking to be happening within the firms on a proactive basis. That is why the provisions for automated decision making within the Bill are so important. We have concerns around whether the more permissive automated decision making approach in the Bill is actually going to lead to greater harms occurring as, effectively, it turns the making of those automated decisions from a sort of prohibition with exceptions into something that, for anything other than special category data, is permitted with some safeguards, which again there are questions around.

Q69 Damian Collins: On that point, just to be clear, as long as what someone is doing is not clearly and purely illegal, legitimate interest means you can do whatever you want.

Michael Birtwistle: Legitimate interest still has a balancing test within it, so you would not necessarily always be able to show that you had passed that test and to do whatever you want but, certainly, the provisions in the Bill around automated decisions bring legitimate interest into scope as something that it is okay to do automated processing around.

Damian Collins: Dr Tennison?

Dr Tennison: On your first point, around the targets of decisions, one of the things that we would really argue for is changing the sets of people who have rights around automated decision making to those who are the subject of the decisions, not necessarily those who data is known about for those decisions. In data governance practice, we talk about these people as being decision subjects, and we think it is they who should have the rights over being informed about when automated decision making is happening, and other kinds of objection and so forth. That is because, in some circumstances, as you said, there might be issues where you do not have information about someone and nevertheless you are making decisions about them, or you have information about a subset of people, which you are then using to make a decision that affects a group of people. In those circumstances, which we can detail more in written evidence, we really need to have the decision subjects' rights being exercised, rather than the data subjects' rights —those who the data is known about.

On the legitimate interest point you raised, there is this balancing test that Michael talked about, that balances the interests of data subjects as well. We think that there should also be some tests in there that balance public interests, which may be a positive thing for using data, but also may be a negative thing. We know that there are collective harms that arise from the processing of data as well.

Q70 Damian Collins: I just want to make sure I have understood that point correctly. Let us say that someone is a recipient of an advert, not because they have been personally targeted, but because they have been targeted through data-matching tools such as lookalike audiences on Facebook. Would that be the sort of thing you are referring to?

Dr Tennison: Yes, it could be, or because they are using a specific browser, they are in a particular area from their IP or something like that. There are various ways in which people can be targeted and affected by those decisions. But we are not just talking about targeted advertising; we are talking about automated decisions in the workplace or automated decisions about energy bills and energy tariffs. There are lots of these decisions being made all the time.

Q71 Damian Collins: Is the gig economy an example of where the systems are biased towards workers who are always available for jobs, or biased towards people based on their proximity to a particular location for work?

Dr Tennison: Yes. Or they may be subject to things like robo-dismissal, where their performance is assessed and they get dismissed from the job, or they are no longer given jobs in a gig economy situation.

Q72 Damian Collins: Effectively a form of constructive dismissal.

Dr Tennison: Yes.

The Chair: I can see Anna Thomas chomping at the bit.

Anna Thomas: I would back up what Jeni is saying about group impacts in the workplace context. It is very important that individuals know how systems are used, why and where they have significant effects, and that risks and impacts are ascertained in advance. If it is just individuals and not groups or representatives, it may well not be possible to know, ascertain or respond to impacts in a way that will improve and maximise good outcomes for everybody—at an individual level and a firm level, as well as at a societal level.

I can give a few examples from work. Our research covers people being told about the rates that they should hit in order to keep their job, but not about the factors that are being taken into account. They are simply told that if you are not hitting that, you will lose your job. Another example is that customer interaction is often not taken into account, because it is not something that can be captured, broken down and assessed in an automated way by an algorithmic system. Similarly, older workers—they are very important at the moment, given that we need to fill vacancies and so on—are feeling that they are being "designed out".

Our research suggests that if we think about the risks and impacts in advance and we take proportionate and reasonable steps to address them, we will get better outcomes and we will get innovation, because innovation should be more than simply value extraction in the scenarios that I have set out. We will improve productivity as well. There is increasing evidence from machine learning experts, economists and organisational management that higher levels of involvement will result in better outcomes.

The Chair: Mr Birtwistle?

Michael Birtwistle: I very much agree with my other panellists on those points. If you are thinking about concrete ways to improve what is in the Bill, the high level of protection around automated decision making is currently in article 22B. That looks at decisions using special category data, which, as an input, you could also add in there, looking at the output. You could include decisions that involve high-risk processing, which is already terminology used throughout the Bill. That would mean that, where automated decision making is used around decisions that involve high-risk processing, you would need meaningful human involvement, explicit consent or substantial public interest.

Q73 Carol Monaghan: Jeni, can I come back to you on automated decision making? You have suggested that a requirement to notify people when an automated decision is made about them would be a useful inclusion in the Bill. Do you think enough consideration has been given to that?

Dr Tennison: The main thing that we have been arguing for is that it should be the wider set of decision subjects, rather than data subjects, who get rights relating to notification, or who can have a review. It is really important that there be notification of automated decision making, and as much transparency as possible about the details of it, and the process that an organisation has gone through in making an impact assessment of what that might mean for all individuals, groups and collective interests that might be affected by that automated decision making.

Q74 Carol Monaghan: We can probably broadly split these decisions into two categories. Decisions are already being made by algorithms online, according to what we are looking at. If I look up a paint colour online, and then start getting adverts for different paint companies, I am not too worried about that. I am more concerned that decisions could be made in the workplace about me, or about energy tariffs, as we have heard. That is more serious. Is there a danger that if we notify individuals of all the automated decisions that are made, it will end up like the cookie scenario—we will just ignore it all?

Dr Tennison: I do not think it is a matter of notifying people about all automated decision making. The Bill suggests limiting that to legally or otherwise significant decisions, so that we have those additional rights only as regards things that will really have an impact on people's lives.

Q75 Carol Monaghan: And you are not comfortable that those have been considered properly in the Bill.

Dr Tennison: I am not comfortable that they are directed to the right people.

Q76 Carol Monaghan: The subject, rather than the decision maker.

Dr Tennison: Yes.

Carol Monaghan: Anna, did you want to come in on that?

Anna Thomas: The last question about the threshold is really important, and it tends to suggest that work should have separate consideration, which is happening all over the world. Last week, Canada introduced its automated decision-making directive, and extended it to work. We have been working with it on that. Japan has a strategy that deals expressly with work. In the United States there are various examples, including the California Privacy Rights Act, of rules that give work special attention in this context. Our proposal for addressing the issue of threshold is that you should always provide notification, assess, and do your best to promote positive impacts and reduce negative ones if the decision-making impacts access to work, termination, pay, contractual status or terms, and, for the rest, when there is significant impact.

Q77 Carol Monaghan: Is there a danger that automated decisions could impact the Equality Act, if biases are not properly accounted for?

Anna Thomas: Yes, absolutely. In our model, we suggest that the impact assessment should incorporate not just the data protection elements, which we say remain essential, but equality of opportunity and disparity of outcome—for example, equal opportunity to promotion, or access to benefits. That should be incorporated in a model that forefronts and considers impacts on work.

Q78 Mike Amesbury: Anna, how would you strengthen the Bill? If you were to table an amendment around employees and AI, what would it be?

Anna Thomas: I would advise very clear additional rights, and a duty to notify in advance what, how and why AI is being used where it has these impacts, and where it meets the threshold that I was just asked about. I would also advise having more consultation throughout design, development and deployment, and ongoing monitoring, because AI changes, and there are impacts that we have not thought about or cannot ascertain in advance.

There should also be a separate obligation to conduct an algorithmic impact assessment. The Bill does nudge in that direction, but it says that there should be an assessment, rather than a data protection impact assessment. We suggest that the opportunity be grasped of clarifying that—at least in the workplace context, but arguably there are lessons more widely—the assessment ought to cover these fundamental aspects, and impacts at work.

Q79 Dr Huq: It is good to see the Ada Lovelace Institute represented; she was a pioneering woman computer scientist who lived in my constituency, so it is a bit ironic that the one man here is representing the institute.

Michael Birtwistle: My colleagues could not be here, unfortunately, but they would have been better representatives in that sense.

Dr Huq: I want to touch on the equality issue again. A 2019 UN report on the digital welfare state made the point that algorithms repeat existing biases and entrench inequalities. How do we get around that? There are a lot of issues around trust and people's rights and protections when it comes to this data. On top of those, there is this issue. Does the legislation address that? How can we overcome it?

Dr Tennison: As I have mentioned, there need to be more points in the Bill where explicit consideration of the public interest, including equality, is written into the sets of considerations that organisations, the ICO and the Secretary of State need to take into account when they are exercising their rights. That includes ensuring that public interest and equality are an explicit part of assessments of high-risk processing. That will help us to make sure that in the assessment process, organisations are made to look beyond the impacts on individuals and data subjects, and to look at the whole societal and economic impacts—even at the environmental impacts—that there might be from the processing that they are looking to carry out.

Anna Thomas: I agree. To add to what I said before, it would help to require a technical bias audit as well as a wider equality impact assessment. One idea that you may wish to consider is this: in the same way that the public sector has an obligation sometimes to consider the reduction of wider inequalities, you could have—well, not a full private sector model requiring that; that may need to be built up over time. We could, at the very least, require consideration of the desirability of reducing inequalities of opportunity and outcome as part of determining our reasonable and proportionate mitigations in the circumstances; that would be easy to do.

Michael Birtwistle: I agree. There is also a question about institutional capability—ensuring that the institutions involved have the capability to react to the use of these technologies as they evolve. Specifically, it would be great to see the ICO asked in the Bill to produce guidance on how the safeguards in article 22C are to be implemented, as that will have a large effect on how automated decision making will be lived in practice and built into firms. The powers reserved for Ministers around interpreting meaningful human involvement, and legal and similarly significant effect, will also have a big impact. It would make more sense for that to be with the ICO.

Dr Huq: Can I add one yes/no question?

The Chair: Yes.

Q80 Dr Huq: If we have an already overburdened regulatory framework, and we put AI on top of it, will it just fall through the cracks? Is there a danger that AI gets forgotten?

Michael Birtwistle: Yes, if regulators are not properly empowered.

Anna Thomas: I strongly agree, but they could be properly empowered and resourced, and in some instances given extra powers to interrogate or to redress what they have found. We advised that there should be a forum in 2020, and are delighted to see the Digital Regulation Cooperation Forum. That could be given additional resources and additional bite, and we would certainly like to see work forefronted and involved in activities. The forum would be well placed, for example, to provide dedicated cross-cutting guidance on impacts in work.

Dr Tennison: I agree with the other panellists. The only thing I would add is that I think that the involvement of the public will be absolutely essential for moving trust forward in those circumstances.

The Chair: The last question is from Chi Onwurah.

Q81 Chi Onwurah: Dr Tennison, could you give an example of the kind of abuse that you are most concerned about taking place if this Bill is passed unchanged, so that we can better understand your concern? And do I have time to ask—

The Chair: You have four minutes.

Chi Onwurah: Great. Ms Thomas, presumably all the automated decisions will be subject to employment law. Would employees have the information they need to appeal decisions and take them to an industrial tribunal?

Dr Tennison: You asked what kind of abuse I am particularly concerned about. I echo some of Anna's concerns around the work context and what that looks like. We have recently been doing some case studies, which again I can share, and they really bring home the kinds of issues that workers are subject to as automated decision making is rolled out in organisations.

More broadly, though, I am concerned about the gradual drift of reducing trust in the public sphere when it comes to the use of data by Governments and organisations. In some ways, I am more concerned about this leading to people not adopting technology and opting out of data collection because they are worried about what might happen. That would hold us back from the progress and the good uses of data that I would really like to see.

Michael Birtwistle: I agree with that very much. We need to think about past public concern around GP data sharing, contact tracing and the Ofqual exams algorithm. When people see their data being used in unexpected ways, or in ways that make them feel uncomfortable, they withdraw their consent and support for that use, and we as a society lose the benefits that data-driven technology can bring.

Anna Thomas: Employment law and the other laws in that context certainly help in some areas; for example, there is unfair dismissal protection, and redundancy protection under the information and consultation regulations. However, it is a patchwork, and it is not clear. Clarity is needed for businesses, to reassure people at work that the principles in the AI White Paper ultimately apply to their data, and to promote prosperity and wellbeing as widely as possible.

The Chair: I thank our three witnesses very much indeed; you have all been fantastic. We are very grateful to you for being here. That brings us to the end of our morning session. The Committee will meet again at 2 o'clock, here in the Boothroyd Room, to continue taking oral evidence. We heard from 10 witnesses this morning and will hear from 13 this afternoon.

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

11.23 am

Adjourned till this day at Two o'clock.