HOUSE OF LORDS

European Affairs Committee

Corrected oral evidence: Data adequacy and its implications for UK-EU relations

Tuesday 26 March 2024

4.05 pm

Watch the meeting

Members present: Lord Ricketts (The Chair); Baroness Anelay of St Johns; Baroness Ashton of Upholland; Baroness Blackstone; Lord Jay of Ewelme; Baroness Hayter of Kentish Town; Baroness Lawlor; Baroness Ludford; Baroness Nicholson of Winterbourne; Baroness Scott of Needham Market; Lord Stirrup.

Evidence Session No. 1 Heard in Public Questions 1 - 16

Witnesses

I: Eleonor Duhs, Partner and Head of Data and Privacy, Bates Wells LLP; Joe Jones, Director of Research and Insights, International Association of Privacy Professionals.

Examination of witnesses

Eleonor Duhs and Joe Jones.

Q1 **The Chair:** Welcome to the European Affairs Committee for the first of our oral evidence sessions for our new inquiry into data adequacy and its implications for UK-EU relations. I am delighted to have our first two witnesses to get us into the subject: Eleonor Duhs, who is partner and head of data and privacy at Bates Wells, and Joe Jones, who is director of research and insights at the International Association of Privacy Professionals. Thank you both very much indeed.

You could perhaps each briefly introduce yourself and your background. I then wanted to ask you a general question, to get the evidence session started, on your assessment of the data adequacy arrangements as they exist now and as they are underpinning the data flows between the UK and the EU. We will pick up all the different aspects of that as we go along.

Eleonor Duhs: Good afternoon. I am a barrister, partner and head of data and privacy at Bates Wells, which is a City of London law firm. Previously, I was a government lawyer. I was the lead lawyer on the GDPR negotiations when I was at the Ministry of Justice. I was also a government EU specialist at the Foreign Office and subsequently at the Department for Exiting the European Union.

The Chair: Joe, perhaps you can introduce yourself as well and then let us come to that first general point.

Joe Jones: Thank you very much for having me today. I am the director of research and insight at the International Association of Privacy Professionals, based in New Hampshire in the US. We are the world's largest information privacy organisation. Our mission is clear: to define, support and improve the profession of privacy and data protection. We have over 80,000 members in over 150 jurisdictions. My role there is to curate and create research that speaks to the work of data protection and privacy, including and especially on international data transfers.

Prior to this role, I was a senior civil servant in DCMS when it had responsibility for data protection and international data transfers. International data transfers was my portfolio there, including with respect to the European Union and other jurisdictions. Prior to that, I was a lawyer at a Washington DC-headquartered law firm, working, again, on international data transfers and digital trade issues.

The Chair: You are both extremely well qualified to help us into this inquiry. Could each of you give us a short overview on how you see the existing data adequacy arrangements and how they are working?

Eleonor Duhs: There are three main points to make here. First, adequacy is of crucial importance to data flows from the EU to the UK. Secondly, it is hugely valued by businesses and there is really significant concern as to what would happen if there was a loss of adequacy. Thirdly,

adequacy constrains what the UK can do in terms of moving away from the EU regime, which in many ways is a problematic regime, because the EU regime has some significant flaws. I do not know whether you would like me to expand those points a little bit.

The Chair: Set them out, yes, and then we will be pursuing them, I am sure.

Eleonor Duhs: In terms of the importance of data flows, you cannot really do business without processing of personal data, from sending an email to a business contact, to putting your customer details on the cloud, to developing new technologies. All of this involves the processing of personal data. The free flow of personal data across borders is crucial to trade across the world. The International Chamber of Commerce has said that the benefits of trade depend on the trusted flow of data between countries. Data transfers are estimated to contribute $11 trillion to global GDP by 2025; that exceeds the global trade in goods, so this really is an important issue.

The free flow of data from the EU to the UK is crucial for the UK economy in many sectors. Examples are banking, finance, retail and hospitality, to name just a few. The free flow of data is important not only for multinationals but also for small and medium-sized enterprises that provide goods and services across borders.

Going to that second point I made, there is real concern about the loss of data adequacy. It comes up when you talk with the data protection community, if I can call it that, about changes to the UK's data protection framework. The first thing everybody asks is whether we are going to lose adequacy as a result. Data adequacy was lost in July 2020 in relation to the US in a case called Schrems II. There was real difficulty and real panic there. That created uncertainty. There is a real concern about not going back to that.

In terms of the constraints on what the UK can do, which is my final point on this, EU data protection law is really complex. The standards are set so high that it really is almost impossible to comply with them. I can expand on that a little later on. The UK's regime currently is almost exactly the same as the EU regime. At the end of the transition period we saved the GDPR into domestic law and called it the UK GDPR.

At its core, EU and UK data protection law is a detailed working out of Article 8 of the European Convention on Human Rights, the right to a private and family life. That human rights core of our data protection legislation is absolutely crucial. It is right to think about it as a fundamental right, particularly in the age of AI. That human rights starting point is the correct one, but the way in which the GDPR translates that right into a set of very complex and unrealistic rules, quite frankly, is regrettable. It needs to be overhauled, but adequacy constrains the UK from doing that in a meaningful way. We need to work with international partners at an international level here. We need an

international treaty on the protection of personal data and the free flow of data.

Joe Jones: I will not repeat but I will second the points made by Eleonor with respect to the importance of the adequacy arrangements. I would emphasise the plurality of those arrangements. These are unilateral decisions from the EU with respect to the UK, but there are also arrangements made by the UK with respect to data transfers to the EU. It is that bilateral combination of the arrangements that is so important to organisations on both sides of the channel and the Irish Sea.

I commend this inquiry because for a long time these issues have been regarded as impossibly complex, and indeed they are incredibly complex and technical, but they are matters of great consequence. These are issues that have escalated and been elevated to head-of-state level. They are matters of high politics and geopolitics. It relates to the information economy that we all live in and how society functions, and of course the pandemic was a sharp reminder about our ability to connect with other parts of the world.

The digital economy depends on international data transfers and it is becoming an increasingly complex web to navigate. Data does not flow across borders like a postcard. It is non-rivalrous in nature. It can be copied, sent and accessed in multiple jurisdictions all at the same time. That makes it very complex for organisations to understand what rules apply with respect to what transfer.

Adequacy is a rather brutal but simple mechanism for organisations. It is essentially an assessment at a governmental level that green lists another jurisdiction. The assessment is done by Governments and regulators so that companies, organisations and the public sector do not need to do that themselves. It is hugely valuable in that respect.

To the question around the assessment of the current arrangements—I am sure we will come on to this later in this session—it is in both sides' interests, the UK and the EU, at a tactical and a more strategic level, for there to be adequacy arrangements in place. That is not just for that bilateral information sharing for the domestic economies. Both sides have wider, more global ambitions and adequacy is an important part of that, but, as Eleonor mentioned, there are constraints.

With the UK having aspirations and ambitions to be more global and fleet of foot than the EU has ever been, that invites concerns and questions about the extent to which the UK might become a back door or sieve for EU data coming to the UK and then subsequently moving to a jurisdiction that the EU has not found adequate. These are just part of some of the various considerations, constraints and questions that are asked presently.

Over the past two years, discourse has settled on these issues. Of course, the timing of this inquiry is important as we head into June next year, when the EU's adequacy decisions will expire or be sunsetted for the UK.

There is a risk, and I saw this first-hand at the time. There is a risk that the discussions on data adequacy become another proxy for the Brexit doomsterism and boosterism and the extremes around the UK's place in the world and the conditions and qualifications it might choose to accept or not accept. The reality probably lies in between those two poles.

To come back and conclude with a point I made at the beginning, these are very technical issues. They are complex. The organisation I work for, the IAPP, runs a global survey of organisations to understand what issues are of most importance and what issues they find most challenging when it comes to data protection. In 2022, we had over 700 responses from companies all around the world. The top issue that they flagged as a strategic priority, concern and challenge that year was international data transfers. It is a very complex set of issues, and increasingly so.

The Chair: To complete the scene setting—I am going to come to Lord Stirrup in a moment for a follow-up—could you say a word about how you see the GDPR functioning at the moment and the 2018 Data Protection Act? We would also be interested in your thoughts on the costs that these regimes are imposing on organisations. That is just a brief point before we get into wider issues.

Eleonor Duhs: One problem, as I have alluded to, is that GDPR is so onerous that it really is almost impossible to be clear that you are complying with it. I heard a story at a data protection conference that somebody was going round wearing a T-shirt saying, "Only God is GDPR compliant". People quote that, but there is a ring of truth to it. No organisation is fully compliant. The concepts are very difficult to understand.

I am indebted to Dr Winfried Veil, who has done some analysis on the burdens that the regime imposes. It imposes 82 balancing tests on organisations including 30 necessity tests that have to be complied with. There are 77 references to the data subjects' rights and freedoms. There is a really serious point here, because having a regime that applies to every organisation in Europe that which no one can properly comply with creates a really serious problem for the rule of law. In a democracy, we should be able to expect that we can understand the law and change our behaviour in order to comply with it. Where you have law that is so complex and onerous that everyone is potentially in breach, that is anti-democratic.

In terms of the costs, there is clear evidence that there are costs that have been imposed by this regime. There has been some very helpful, recently published research on this by Frey and Presidente, published in 2024, entitled *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*. It says that the digital technology companies have been most impacted by GDPR. Technology companies that were targeting EU markets have experienced a 2.1% reduction in profits. The GDPR also increases non-operating costs as well as firm wage bills. They also cite previous research on the impact on SMEs, which says that they face

significant challenges due to GDPR across various dimensions and that smaller companies have suffered more in terms of profitability.

I would weigh that against the cost of not investing at all in data protection compliance, where, if you do not invest, there will be no real sense of trust from consumers in how their personal data is being used. There is a lot of evidence that that is something that people are worried about. Elizabeth Denham mentioned it in the response to the Government's consultation, *Data: a New Direction*. If people do not trust how their data is being used, they will not turn it over and then we will not be able to develop these new technologies that we are so keen to develop.

Dr Jeni Tennison also made a similar point, giving evidence in the House of Commons about the Data Protection and Digital Information Bill. She said that she was very worried that there is a lack of trust and a drift towards reducing trust in the public sphere when it comes to government and organisational use of data. She said, "That could hold us back from the progress and the good uses of data that I would really like to see". So it is expensive, but it is also important.

Joe Jones: May this year will mark eight years of the text of the GDPR being settled and six years since it first applied. Despite, or perhaps because of, its age, there are still remaining many areas of complexity and confusion. Without a doubt, it has become the global model. Countries have not just taken inspiration from it. Many countries have quite literally taken the words from it and supplanted them into their own regime, but it is not without controversy, confusion and complexity. Just last year, 5% of all of the cases that went to the European Court of Justice were to clarify aspects of the GDPR. I suspect that is probably a factor relating to parts of its interpretation and application that may go beyond what was originally intended many years ago in 2012, when it was first proposed.

Of course, we have lived through some seismic moments that have shifted the paradigm on our understanding of how data is accessed, collected, used and protected. There was the pandemic and, in today's era, the rapid implementation and acceleration of artificial intelligence. So there is a lot that remains challenging. It has been a global model, and not just for lawmakers and policymakers; a lot of large multinationals have, in effect, benchmarked themselves to the GDPR wherever they are in the world, including in jurisdictions that do not have data protection and privacy laws. That speaks to some of the legacy.

To your point on cost, it has become not just a cost of doing business, but, to Eleonor's point, a worthwhile cost for many. Discourse has moved away from seeing these issues as zero-sum and more around how we can leverage the fact that we have good privacy and data protection to earn the trust, and in a way that is good for business and public sector delivery of services.

Q2 **Lord Stirrup:** You said that there was a panicked reaction to Schrems II.

I cannot remember whether you used the word "panic", but that was the sense I got. Could you very briefly tell us something about the nature and scale of the actual harms that ensued?

Eleonor Duhs: On the day that Schrems came out, I think the Berlin regulator put out a press release saying "Data flows to the US must stop now". Everyone thought, "Oh gosh, how am I going to run my business?" It really was a panic.

The European regulators—of course the UK was part of that bloc at the time; it was during the implementation period—tried to help. The issue was that not only was the adequacy decision for the US invalidated, but the court said that, if you wanted to transfer data to a third country, not using adequacy but using standard contractual clauses—something like 96% of data transfers use those standard contractual clauses as an alternative to adequacy if it does not exist—not only would you have to put those in place but you would have to do a transfer risk assessment. You would have to look at a whole series of things that the European Commission has to look at when it confers adequacy, such as adherence to the rule of law in the third country, human rights, legislation, both general and sectoral, including national security legislation, defence and public security, and whether the country in question has an independent regulator.

This is an almost impossible task. It was a difficult enough task for the European Commission to do and the Court of Justice has said twice, "You have got it wrong". Having to do those sorts of analyses at scale and at pace to keep those data flows going was something that businesses really struggled with.

Lord Stirrup: What was the impact upon US-EU trade?

Eleonor Duhs: I am not sure what the figures are, but there was real concern that you could no longer send personal data to the US because of the way in which the judgment had been worded. People came back from that position pretty quickly and I think the Berlin regulator was told that that was just a press release and it should not have been put out in that way. As I said before, this is a regime that everyone fears they are in breach of, and the impact was that everyone felt, "Do we have to choose between continuing to trade with the US or stopping the data flows?" People continued with the data flows, but there was a lot of work to do to try to make sure that those were still lawful.

Joe Jones: To add to that, there were instances where organisations threatened to pull out of the European Union because of the costs of doing business, especially where that business was not just data-driven but dependent on sending data back to the United States. There was a perception and a sense of anxiety as to the efficacy and longevity of doing business in the EU and offering products and services in the EU.

To compound that, there were various more localised instances where some regulators in the EU expressed a preference and/or issued orders

for local data storage and localised processing of data. Data could not leave the jurisdiction, in essence creating this fort around the data flows. To the point I was making at the beginning, that poses serious operational and cost challenges for organisations, especially those small organisations that depend on US-based service providers, whether that is cloud computing, email providers or using Microsoft Teams, et cetera.

Q3 **Baroness Anelay of St Johns:** Good afternoon. Both of you referred to the complexity of GDPR and the fact that people get very concerned that they may not be compliant and the regulator will take action. My questions are about the UK's regulator, so it is about the Information Commissioner's Office. That office not only has to deal with GDPR, a major part of its work, but with the Environmental Information Regulations and FoI, about which all of us around the table today have experience, I should imagine. With that workload and the complexity you have alluded to, how would you assess the overall performance and effectiveness of the UK's current regulator? Has the regulator's performance been affected by the decisions that have been made on data adequacy? If so, how?

Eleonor Duhs: The regulator has a very high reputation internationally. When the UK voted to leave the EU, some EU lawyers—these were data protection practitioners—said that they were very upset. They said that the Information Commissioner's Office's guidance was so practical and helpful; it really helped to translate these very complex concepts for them. So its reputation is very high, as I say.

In terms of my experience of having clients who have received complaints that have been taken to the ICO, when case officers at the ICO have looked at those issues, they have been extremely thorough. I have been really impressed with their grasp of the regime. Their approach is usually thoughtful. It is pragmatic. If there has been non-compliance, they will take that pragmatic approach and usually advise an organisation how to get it right and improve its compliance. That is the way that most cases are disposed of.

There are some issues with that, though. There has been some research by Professor David Erdos at the University of Cambridge, which highlights what some consider to be evidence of a poor track record of enforcement. In 2021 to 2022, the ICO did not serve a single GDPR enforcement notice, secured no criminal convictions and issued only four GDPR fines, totalling £633,000[1], despite the fact that it had received over 40,000 data subject complaints. That may be partly because of the difficulty of complying with the regime. So there is a mixed picture.

I do not know about the impact of the adequacy decision on the workings of the ICO, because I am not familiar with the internal workings. The guidance following the Schrems II case was extremely pragmatic, very

[1] Ms Duhs has later clarified that the final 2021-22 figures were even lower than cited as the Information Commissioner's Office reduced one of the four fines giving a total final figure of just £183k total & no enforcement notices or convictions.

well reasoned and has really helped to make international data transfers less onerous for UK businesses, so that is very welcome indeed.

Joe Jones: It is very hard to assess and/or compare the efficacy of the data protection authorities, principally because it is hard to identify a useful measure or metric. Is it the amount of fines that have been issued or the amount of criminal convictions? Much of that is dependent on the local circumstances, who is bringing the case and on what. For that reason it is hard to compare. It is apples and oranges in many cases. If you were to apply that to the EU, you would see that the Irish regulator and the Luxembourg regulator are those that are issuing the fines. That is for reasons other than their propensity and desire to issue fines. It is because companies are headquartered there.

To the point around the impact of a no adequacy or limited adequacy scenario on the efficacy of the ICO, I do not think that there would be a direct impact, because the ICO, as I understand it, is not receiving EU data in a way that many businesses in the public sector would. However, there are two potential indirect impacts that might occur. The first is that—we saw this with the Get Ready for Brexit campaign—a lot of ICO resources would divert and be moved to assisting UK organisations to get ready for a potential scenario where there is no or limited adequacy. That might beg the question, "At what expense and at what opportunity cost are those resources being diverted there and from where?" That is one potential indirect impact.

The other is general mood music. The UK having adequacy from the EU serves as a helpful badge and helpful designation when the ICO goes about its business, looking to co-operate with other regulators not just within the EU but around the world. Recently, the ICO has concluded various memoranda of understanding with international regulators, including regulators within the EU at a national level and at a pan-EU level. This is conjecture, but I suppose it would be helpful mood music to have that governmental legal acknowledgement that the regulators in these different jurisdictions are operating under equivalent regulatory frameworks.

Baroness Anelay of St Johns: Can I follow up with a question that refers to the Data Protection and Digital Information Bill but does not encroach on later questions? I have tried hard. I am very intrigued by the way in which you have told us that the GDPR work here is actually admired from the point of view of the work of the Information Commissioner's Office. The Data Protection and Digital Information Bill does reflect changes that were discussed during the 2021 consultation, including that, instead of being corporation sole, it should move to a commission status. Do you see that as a way that is going to assist its work or not? I am interested from the point of view of the structure and functionality of organisations.

Eleonor Duhs: I do not have a particular view on that, I am afraid. It is quite a change. There are other regulators, such as the Financial Conduct

Authority, which have a board, but I am afraid that I do not feel qualified to answer that question.

Joe Jones: I feel likewise. It brings the ICO into line with practices that exist elsewhere, not just in the UK but around the world. I mentioned Ireland. It has commissioners. Australia has commissioners and more delegated responsibility. Some of that speaks to greater resilience at a decision-making level as well, but it would be conjecture for me to opine on the efficacy of what that might mean going forward.

Q4 **Lord Stirrup:** You have already referred to the fact that the data adequacy arrangement is up for review next year. I realise you cannot speak for the EU, but we would value your opinions on what factors the European Commission in particular would be considering when deciding whether to renew the arrangement and what sort of weight it would give to the various factors. Particularly in light of what you described under Schrems and the turmoil that caused, what would be its approach and the key factors it would be looking at?

Eleonor Duhs: I think that there would be a very different approach from the European Commission compared to if there was a challenge before the Court of Justice. I think that we are going to come on to that.

Lord Stirrup: That is the next question.

Eleonor Duhs: **T**he European Commission would do everything it could to continue data adequacy for the UK. EU businesses will want to be able to send data freely to the UK without having to put standard contractual clauses and risk assessments in place.

Also, one of the issues for the European Commission is that, if the UK does not have adequacy, the bar is set almost impossibly high for any other country. Even with the Data Protection and Digital Information Bill, our data protection framework will be very similar to the EU's. That also creates some risk for the UK, because it is very evident where the UK is dropping its standards. None the less, I think that the European Commission would take a very pragmatic decision.

It is also worth noting that the European Commission's approach to adequacy is very strongly political. There is a Commission communication of 10 January 2017 that sets out criteria for the Commission to consider when deciding whether it should enter into a negotiation for adequacy with a third country. Those include the extent of the EU's commercial relations with the third country, the extent of personal data flows from the EU to the third country, reflecting geographical or cultural ties, the role of the third country in the field of privacy and data protection and the overall political relationship with the third country in question. All of those are very important in reviewing the UK's data adequacy decisions. I have no doubt that the European Commission will do everything in its power to keep data flowing.

Joe Jones: The European Commission's assessment of the UK is quite unlike any of its other assessments and it will forever remain so, because

the UK was assessed as adequate at a point in time when it was operating under a nearly identical framework. All other jurisdictions—I think we will come on to this later—have been converging closer to EU standards. In the words of the European Commission, the UK is a jurisdiction that has started so close but purports to diverge.

To your question, the focus of the European Commission's assessment will be narrow and focused on that delta. What is the difference? What is the substance of the protections that have been regulated for to diverge? What does that mean in practice?

In terms of the EU, there is the European Commission, the Court of Justice and the other institutions. There are laws on the books, and that is important: what does the law say? I really think that the focus of adequacy assessment is how the law is working on the ground. What has it resulted in in terms of a pattern or culture of compliance? Is the regulator effective? Are we seeing meaningful practices? That will be the focus: the delta of difference between the UK as it was at the end of June 2021 and where the UK is—not where the UK might be heading—at the point in time it is assessed next year.

Q5 **Baroness Ludford:** Could I indulge in a couple of comments before I ask my actual question? The first is that, having played a minor role in the GDPR a decade ago as an MEP, if you think that the end result was prescriptive and complex, you should have seen the first draft from the European Parliament rapporteur that some of us had to work on to try to get a bit more balance and pragmatism. Clearly we did not succeed to your satisfaction, but there you go.

The second thing is that Eleonor talked a lot about the costs and Joe used the phrase "worthwhile cost" and talked about an investment in trust. The NHS is a good example of loss of trust, because of the casual and careless way a decade ago it introduced the opt-outs on use of medical data. It has struggled ever since to get trust and confidence of patients in the use of medical data. I say that with a heavy heart, as someone who cares about medical research. Forgive me that indulgence.

My question is about the European Court of Justice. Eleonor is quite right that the European Commission will strain every sinew to keep data adequacy and will look at the economic relationship, but the ECJ will not do that. One thing that has long bothered many of us is the national security dimension and this peculiar double standard, as one commentator called it. When you are inside the EU, whatever the ECJ has said about UK intelligence and data collection, it cannot do anything about it, but when we are outside we are assessed on a much higher standard. If there is a Schrems III, what factors do you think the ECJ would consider if the legality of the UK data adequacy decision was challenged in court?

Eleonor Duhs: The CJEU would look at whether the standard of protection of personal data in the UK was essentially equivalent to that in the EU. There does not have to be a carbon copy, but the standards have

to be essentially equivalent. The UK is at a disadvantage here because, if our law was completely different from the EU's, it would be much more difficult to say that it was or was not essentially equivalent. It is very clear, because it is so similar, whether the standards have dropped.

There are four areas of risk that are worth mentioning that the Court of Justice would be concerned about. If the Data Protection and Digital Information Bill goes through as drafted, there will be more. There are four areas I would like to briefly highlight.

The first is the standard of protection for data subjects since the Retained EU Law (Revocation and Reform) Act came in at the end of last year. Also through the Retained EU Law (Revocation and Reform) Act there is the deletion of the concept of EU fundamental rights, and with it the right to the protection of personal data and potential loss of Court of Justice case law in the area of data protection, which is really quite significant.

The independence of the regulator is something that is in the Data Protection and Digital Information Bill, but it is so important because it is set out in the Charter of Fundamental Rights. That is something that the CJEU would be very conscious of. Finally, there are the UK's obligations under international law, both adherence to the ECHR and Council of Europe Convention 108, which is a Council of Europe treaty from 1981 on data protection.

To expand those four points briefly, the first is the dropping of the standard of protection for data subjects. Currently, the position is actually that data protection rights for migrants in the UK are stronger than for any other group. The reason for that is that there was a challenge brought after the implementation period but while we had retained EU law in place. The challenge was based on exemptions for immigration purposes being too broad. The Home Office has been forced to apply a substantial number of safeguards where data subjects who are migrants are concerned.

That sort of challenge has now gone, from the end of last year. It is very likely that, if the Court of Justice looked at the exemptions for every other group apart from migrants, it would say that they were lower than the EU standard, because this challenge was an EU-style challenge that now no longer exists. It is very clear that the level of protection of personal data for individuals other than migrants is lower than it would be in the EU. It is quite important to note that the UK did not get adequacy for the area of immigration because of this challenge, because there was a question mark over whether the standard of protection was sufficiently strong. It just happens that no other challenge was brought at the time, but that is an area where data protection rights are now clearly lower in the UK than in the EU.

Going on to the effect of the Retained EU Law (Revocation and Reform) Act in the context of fundamental rights, the area of fundamental rights is the underpinning foundation of the GDPR. The first recital says that this is an area of EU fundamental rights. Those have been deleted from the end

of last year through the Retained EU Law (Revocation and Reform) Act. The Government, realising that this was quite problematic, brought forward some secondary legislation at the end of last year to say, where you look at the concepts of fundamental rights and freedoms in the UK GDPR, that should now be read as fundamental rights and freedoms in the ECHR, particularly Article 8 of the ECHR, the right to a private and family life.

There is a real question mark as to whether the right under the ECHR is as protective as the right under the EU legal order. There is a case of Watson from 2015 that says that EU fundamental rights go further than ECHR rights and are more specific. That is an area of worry that the Court of Justice might look at. With that, potentially, we have lost the case law of the Court of Justice on some very important areas, including Schrems. The Court of Justice looks at the EU data protection framework through the prism of EU fundamental rights, so this is a very important issue for EU adequacy continuing for the UK.

The independence of the regulator is absolutely key in data protection law. It is mentioned in Article 8 of the Charter of Fundamental Rights. Article 8(3) says that compliance with data protection rules should be controlled by an independent authority. One thing that the Data Protection and Digital Information Bill does is that, in the new test for adequacy, it removes the need to look at whether the third country that you are assessing has an independent regulator. Given the very prominent role of the charter—the charter has the same standing as the EU treaties—if the UK is moving away from that concept of independence of the regulator when looking at whether third countries are adequate, the Court of Justice would be very concerned about that.

My final point is about international commitments. Recital 19 to the UK's current adequacy decision highlights that the UK's adherence to the European Convention on Human Rights and the Council of Europe Convention 108 is, according to the drafting, a particularly important element of adequacy. If the next election were fought on a manifesto to leave the ECHR, that would have consequences for adequacy and the free flow of data if there was a challenge before the Court of Justice.

Finally, on Council of Europe Convention 108, that convention has been modernised to reflect GDPR standards and the UK has not ratified that convention. Professor David Erdos of Cambridge, who I mentioned before, thinks that that modernised version of Council of Europe Convention 108 will enter into force in the next two years. So, again, if the UK does not ratify the modernised convention, that supports arguments that that test of essential equivalence is not being met.

The Chair: Can I do my chairman's thing and say that we are only about half way through our questions? It is so fascinating that we are taking up quite a lot of time. I hope, first, that you might be able to stay a little bit more than the hour, so we can cover all the ground. Secondly, can we try to be as concise as possible, please, so that we can get to all the questions in what is a really important evidence session? Sorry about

that.

Joe Jones: I will briefly add to the question. If the test is essential equivalence, that test is very hard to apply in the context of national security, because you must complete the test. What is it essentially equivalent to? It is one thing to apply that test of essential equivalence when you are comparing the GDPR with the UK GDPR, or the independence of European regulators with the independence of the UK ICO. It is quite another to apply that test in the domain of national security and law enforcement. That is something that is the preserve of the member states.

There is great variety among the member states when it comes to the safeguards that exist in law and in practice as concerns the ability of their authorities to access personal data held by companies, to subsequently process that personal data, and then the rights to recourse and remedies that exist. It is a very hard equation to solve for the Court of Justice.

In the first Schrems case and in the Schrems II case, we saw from the Court of Justice what was not good enough. In both cases the United States was ruled to be wanting in aspects of safeguards concerning national security. We do not yet have an articulation by the court as to what the standard should be, what the practices should be and what the law should say. There has been a lot of work at a policy level, at the OECD and elsewhere, to try to articulate what "good" should look like, but it will be a very challenging set of questions for the Court of Justice to ask itself and to subsequently answer. We have the investigatory powers regime here in the UK. Is that essentially equivalent to the laws and practices that exist in the EU, looking at what exists from Hungary to Portugal? That is going to be a very hard set of arguments.

Q6 **Baroness Blackstone:** You have already made some reference to the Data Protection and Digital Information Bill that is going through Parliament and is still in the Lords. I wonder whether we could start with Joe Jones on this one, because he has not referred to it whereas you did at some length. Can you tell us whether you are reasonably happy with the policies that it sets out and whether you think there are any issues that it raises as far as greater divergence between the UK and the EU is concerned?

Joe Jones: These will certainly be my personal views informed by my experience, rather than those of the IAPP. My strong sense is that the reforms have been designed with a view to retaining EU adequacy. The question the Government are asking themselves is, "We have inherited the GDPR. For all the reasons we have said, there is some complexity and confusion. How do we add clarity to that and how do we do so in a way that presents gain?" Despite, or maybe in spite of, all of the confusion, organisations have by and large got used to the GDPR. It has been around for eight years. That is a tricky balancing act.

The Bill is lengthy and complex, despite its aims to add clarity. There are various opportunities or options for organisations to avail themselves of

less paperwork and less administrative burdens when it comes to filling out impact assessments and appointing statutorily prescribed roles—but they may still choose to comply with the EU GDPR. That is a policy choice that has been codified in the Bill: that organisations do not have to move away from EU GDPR. That option, though confusing, is broadly welcome because organisations invested a huge amount of money to comply with the GDPR. Making nips and tucks for one country when they might have a GDPR approach globally is not always a straightforward exercise.

There are certain aspects there that some organisations will avail themselves of, in particular the requirements around paperwork. Government is working closely with the European Commission to understand how far it could go on certain aspects without falling foul of EU adequacy.

Baroness Blackstone: Can I follow up on that? If they are working closely with the European Commission, is there then not really a threat with respect to greater divergence? I think that one or both of you implied that there is such a threat. If there is, why have the Commission and the UK Government not been able to avoid it? Could you illustrate where these threats are and put some flesh on it for us?

Joe Jones: My own view is that a lot of the threats lie outside of the Data Protection and Digital Information Bill. Within the current parameters of what is being considered and proposed in that Bill are things that do not go to the heart of essential equivalence. Perhaps I am putting emphasis on the essence of equivalence.

The greater threats are those threats that are perceived to exist outside of the Data Protection and Digital Information Bill, such as proposals and policy discussions that relate to the wider regulatory environment, the commitment to the rule of law and the adherence to international laws and treaties. Those are the issues that I believe that the European Commission will be most seized of. Then there is the set of questions and issues relating to how public authorities can access personal data for national security and law enforcement purposes. We have a rich history in this country of proposing laws relating to investigatory powers and having to revise those. That will be something that will be litigated and subject to scrutiny.

Q7 **Baroness Nicholson of Winterbourne:** My question is about the risk of the EC withdrawing the UK data adequacy decision. I think that you both inferred that you think that that is very unlikely. Am I correct on that?

Maybe I might just pop something else in. There is an implicit assumption in the way that the subject is being discussed that there is a special partnership between the European Union and Council of Europe conventions, yet my recollection on some work, particularly on the children's issues, is that in fact the UN convention also comes in. I wonder whether at one point we might have a careful look at the way these things impact on each other. For example, on the data protection for children's rights, in the end the European Commission declared that

the convention from the UN overruled everything. We have that in the judgments there.

I wonder whether we are being a little bit too narrow today and not looking quite deep and wide enough on some of these things. The UN Convention on the Rights of the Child is still the most significant and detailed convention of the whole lot. That impacts on a number of laws and rulings. That third intervention might very well be worth having a very careful look at when we have a look at this in general in our report.

The Chair: Would the panel like to pick up Baroness Nicholson's challenge about thinking more widely to embrace the UN conventions as well?

Joe Jones: It is a good point and well made, because the European Union is not just involved in but is an advocate for a number of those initiatives. There has been a real proliferation in multilateral policy-making and agreements on data privacy, data protection and wider digital governance issues, whether that is specific to children, other vulnerable communities or across the board. All of this comes out in the wash together.

Baroness Nicholson of Winterbourne: My point in raising it was that our underlying view in the UK is always the rights of the individual, and therefore the UN conventions should be taken into the context as well. The rights of the individual are a common-law priority in a sense, as are the rights of the family and so on.

Q8 **Baroness Ludford:** We have largely been talking about business data transfers, but could I ask you about policing and justice? What do you think would be the implications of any disruption to data adequacy for the continued operation of part 3 of the trade and co-operation agreement, focusing on law enforcement and judicial co-operation on criminal matters?

Eleonor Duhs: Article 693 of the trade and co-operation agreement says that, if adequacy is lost, part 3 could be suspended, which could affect co-operation on matters such as cross-border crime and terrorism, extradition, passenger name records, criminal records, criminal justice, mutual assistance and cybercrime. Obviously, that is extremely important.

I should also mention briefly that Article 71 of the withdrawal agreement would also be relevant here, because the UK and the EU have agreed that, if the UK loses adequacy, personal data that came from the EU, either during membership or during the implementation period, should continue to be protected to essentially equivalent GDPR standards. So we would have a two-tier system here in the UK, where EU data would have to be treated differently from UK data. That would cause real operational issues.

Q9 **Baroness Hayter of Kentish Town:** This is very small. That only mentions criminal justice. What about the data for civil justice, particular

family? Is that affected by this at all?

Eleonor Duhs: I am not aware that that suspension would happen in the same way as it would under part 3, but I am afraid I have not looked at those provisions in detail.

The Chair: Let us move on to the last sequence of our questions, on the important issue of the wider world and other areas of good practice and so on.

Q10 **Baroness Scott of Needham Market:** Good afternoon. We are not entirely working in the dark here. The Commission has carried out reviews in 11 countries. What are your conclusions about their approach to those reviews? What are your conclusions about how their thinking might impact on how the UK behaves going forward?

Eleonor Duhs: The reviews are interesting because they emphasise that data adequacy, for the Commission, is political rather than legal. The evidence suggests that the Commission is not really ensuring that its legal tests for adequacy are met. Those are aspects such as the rule of law, respect for human rights and fundamental freedoms, access of public authorities to personal data, the implementation of their legislation, and effective administration and redress for data subjects whose data is being transferred.

I have one example, which is Argentina. If you read the adequacy decision, there is an awful lot of analysis of the law in Argentina, but, if an organisation is going to transfer personal data without an adequacy decision, it is required to look at reports of what is happening in a jurisdiction in relation to the rule of law, human rights and that sort of thing.

I had a look at a US State Department report on Argentina in 2022, which said there were significant human rights issues, including reports of unlawful and arbitrary killings and extrajudicial killings; torture, cruel, inhuman and degrading treatment and punishment by federal and provincial officials; harsh and life-threatening prison conditions; serious problems with the independence of the judiciary; serious government corruption; and the Government taking limited steps to identify, investigate, prosecute and punish officials who have committed human rights abuses or engaged in corruption.

So there is a huge disparity between what you see written about the rule of law in these countries and what sadly appears, from the point of view of the US State Department, to be happening on the ground in those jurisdictions. Again, that speaks to the political nature of the European Commission's assessment rather than a strict application of those legal tests.

Joe Jones: I would add that it is not all art; there is some science here. The reviews into the 11 jurisdictions go over 350 pages. There is some robust argumentation there as to whether, why and how those countries still meet the test. The test is specific to the risks that attach to when

data is transferred. It is not an assessment of the country writ large. It is an assessment of those countries' protections that are relevant to data that is transferred there. That is both narrow and broad, for the reasons that we are discussing today.

The European Commission's report says a few things. It speaks to its commitment to continuity, to continue all of those arrangements that exist. It speaks to its global perspective and strategic ambitions in this space: to promote the free flow of data where there are strong protections rather than being in the business of cutting the cord and stopping data flows, even though there might be reasonable arguments to suggest that you might want to do that in some cases.

The report does show that in all 11 instances—I would add Japan as well because they were reviewed via a separate process last year—there have been improvements since the original assessment. That goes to the point I was making previously around how the countries and jurisdictions that the European Commission has been assessing when it comes to data protection are converging closer and closer to EU standards.

Examples include the independence of the regulator, codifying rules around reporting data breaches, incident reporting and the appointment of dedicated personnel. The introduction of data protection officers is a proposal that is currently under consideration in Israel, for example. So you are looking at a basket of jurisdictions that are getting closer, not further apart. That really speaks to the uniqueness of the challenges that will be faced on both sides of the channel next year.

Q11 **Baroness Ludford:** There is one thing that is concerning me. Last autumn, the European Parliament's LIBE Committee made a pretty chilly assessment of the UK on various aspects, including data protection. There will be hearings after the European elections for the new candidate commissioners. Data protection is always a subject for the European Parliament, but, on this particular theme, the renewal of UK data advocacy could come up. Is that on your radar at all?

Joe Jones: I am certain it has come up. There is a long lead-in period to these moments. The decisions expire at the end of June 2025. I would suspect—I would not bet on it—that conversations are already happening at political levels and working levels with respect to the renewal of those decisions.

Q12 **Lord Jay of Ewelme:** I have one general question to start with. It really picks up on something that both of you, particularly Eleonor Duhs, said earlier on, which is the problem of complexity and indeed the possible implications for the rule of law and the application of the rule of law. The answer to this may simply be a straightforward "no". Is there any possibility of greater simplification as time goes on?

Eleonor Duhs: That would be a huge advantage. How we protect personal data is such an important issue, particularly in the age of AI. We cannot simply keep legislating faster and faster, with more and more legislation, to try to keep up.

We need to go back to some really key principles and outcomes for what we want to see. That should be in legislation. We then need detailed guidance on how that translates into these new technologies. We need that guidance to be drafted by well-resourced and independent regulators. That is the answer. Of course, we need an international consensus on what these principles and outcomes should be, but that is the way forward.

Lord Jay of Ewelme: Is it just you who thinks that or do others think that too?

Eleonor Duhs: Others think that, too. I was at a conference in Cambridge on Friday. There were an awful lot of us agreeing on all of this.

Lord Jay of Ewelme: That was just a one-off question. Joe Jones already made the rather good point about Britain starting from a position of equivalence and moving away from it or wanting to move away from it. Other countries are moving quite a long way away from it and trying to get together. Does that mean there are no lessons to be learned by us from what other countries are doing? Are there things that other countries are doing that would be quite useful for us to learn from?

Joe Jones: There absolutely are lessons to be learned, including from those countries that are in receipt of EU adequacy that are none the less reforming or revising their frameworks in ways that are different from the EU GDPR. That does exist.

Canada is a good example of a country that, in some respects, has quite different rules and requirements from those that exist under the EU GDPR, but it is adequate. Examples include the Canadian rules on international data transfers. They do not do adequacy in Canada. Instead, the requirement is pushed down to organisations to agree at a contractual level the protection that attaches to data when it is transferred.

To your point around the growing complexity, just picking on this Canadian example, today we are talking about UK-EU data adequacy. We have mentioned the United States, and we have that triangle of data transfer arrangements. This is a global challenge for organisations and policymakers. There are 84 jurisdictions, in addition to the EU, that assess other jurisdictions for adequacy. That is a hugely complex web to navigate. Many of those jurisdictions have not found anybody adequate. They have these laws on the books, but they are not using them.

Then you have issues about the gaps and the overlaps between the different frameworks. It is very complex for organisations operating in the 84 plus the EU market to understand who is on whose list and what the repercussions might be if we send data to a country that is on their list but not on the other one. That is very complex to navigate and to comply with.

There is a tide coming in; there is a focus from policymakers and lawmakers to try to connect those dots. The EU will refer to it as the network effect. Some of the 84 do not do their own assessments. They take the EU's. They will say, "Whoever the European Commission says is adequate, that is fine by us". Others are trying to come up with more multilateral agreements. Those are not unilateral in the sense of, "I assess you and you assess me". They are much more codified; they are almost like a treaty. There are various initiatives, which we will come on to later, that reflect that.

Lord Jay of Ewelme: I ought to know this, but I do not. What is the position between the EU and Canada at the moment? What is the relationship on data adequacy at the moment?

Joe Jones: The EU has designated Canada as adequate.

Lord Jay of Ewelme: That is despite the fact that it does not have an adequacy approach.

Joe Jones: Despite the fact that it does not have its own ability to assess the adequacy of others, it still none the less has safeguards for international transfers. Those safeguards are just contractual.

That adequacy decision for Canada is partial. It applies to the private sector and not the public sector. That is an arrangement that the EU has also concluded with Japan. The European Commission has a track record of proposing and concluding surgical fixes that work for what is adequate and what is not adequate. A sectoral adequacy decision is a good example of that.

Q13 **Baroness Lawlor:** First, I am so sorry for being late and missing some of what you said. I had an emergency to deal with that just could not be delegated.

I am very interested in what you have been saying about the complexity of arrangements. Everybody is agreed that consumers want and need protection—this is a market aim of everybody—and that data must be kept secure and private. I do not know that any jurisdiction would not agree with such aims and seek to promote them.

To what extent do those third countries that trade with the EU and are deemed or not deemed to be EU-adequate have laws designed to promote those same principles? Why would they not be adequate, if they do?

My supplementary—you can think about it—is that, from what you have said about the enormous complication in data protection and the potential for even more complex legislation, it seems that something will have to give. Businesses cannot keep up with these laws.

As you were talking, it struck me that we are talking about a difference in the approach to law. The EU approach to law is code-based. It seeks to cover every single potential problem with a code or a direction. The UK's law is more based on making a law and ensuring that it provides for

breaches so that consumers and other people can have satisfaction if their rights under the law are breached. That is left to the courts. In a way, our law is completely unpolitical. It judges on the basis of the evidence, whereas the EU's arrangements, as you say, are political. They are very much linked to the aims of the EU. Indeed, that was part of its founding pillars way back in the 1950s.

How do you see those third countries that are not in line with necessarily EU data adequacy but have their own equivalent arrangements continuing their relationship with the EU? Is there any scope for the EU to move to a more business-friendly model that can be understood? In the end, as Eleonor Duhs has said, the law must be respected and it must be transparent to be respected. People must know what is involved. How do you see things going for third countries, including the UK, if we are deemed not compatible with data?

Joe Jones: Speaking from experience, the assessment of adequacy is arduous. It is resource-intensive. To do it well at scale requires acknowledging that issues related to privacy and data protection are inherently reflective of legal and societal cultures and traditions. To pierce the veil of the differences that exist across jurisdictions is a hard exercise.

Countries in Asia-Pacific and south-east Asia have a very different approach that reflects their way of doing law and their strategic outlook. They will perhaps share all of those objectives that you outlined around wanting to protect data here and overseas, but they might go about it very differently, through standards, codes of conduct or multiple sectoral regulatory initiatives.

The United States is a good example. There are 137 countries in the world with national data protection laws. The United States is not one of those, but it does have numerous sectoral laws. Indeed, many of the states have comprehensive privacy laws.

It is challenging, as the assessor, as I said, to pierce that veil of, "They do things very differently to us, and we must now compare apples with oranges and come up with a conclusion on whether they are adequate". It takes a long time. The adequacy function has existed since the 1995 data protection directive. To date, 16 jurisdictions are adequate. Hundreds of pages of reports have been generated to evidence the adequacy. This is a resource-intensive exercise, which is very legal and very technical. In order to scale, it will require lots more effort, some imaginative and creative policymaking and perhaps multilateral initiatives as well.

Eleonor Duhs: We need to bring the EU with us in this dialogue. That is so important. We need an international consensus, and we need to work really hard to make a model that allows trade to happen but respects people's fundamental right to privacy. The importance of trust in that framework is absolutely crucial. There are no easy solutions here. It really does require an awful lot of political will and pragmatism.

Baroness Lawlor: Given that it is a comparatively new area, is it more likely to be able to modernise in line with what in fact is being regulated, digital trade?

Eleonor Duhs: In some ways it is not such a new area; it is just that we have these new technologies. The right to private family life goes back to Article 8 of the ECHR. That is where we need to start.

It is important that we translate those very flexible principles into legislation in a way that people can really understand and comply with. This is not an absolute right. The right to privacy is not absolute; it is qualified. We need to think very hard about how we qualify it in order to facilitate those very important things such as trade and business.

Q14 **The Chair:** Thank you very much indeed. I am conscious that we have taken an awful lot of your time. I have one more specific question and then I was going to turn to Baroness Hayter for an extra-time question.

You have mentioned the other multilateral frameworks. An obvious one is the global cross-border privacy rules, built on the APEC system. The UK is now an associate member of that. If the UK decided to become a full member of the global rules framework, how would that impact on UK-EU data adequacy?

Joe Jones: There is an assumption there that I would like to correct. The global cross-border privacy rules are not designed to remain as they are presently. The intention of the full members, and indeed the intention of the associate members, presently just the United Kingdom, is to revise, reform and update the cross-border privacy rules. In some respects it is an assessment of a future state, but we do not quite know what that state looks like.

Without a doubt, the European Commission has been critical of the APEC cross-border privacy rules. The standards are there, but the European Commission has been so critical that, in its adequacy decision for Japan, it explicitly carved out of scope the APEC CBPRs. The Commission said that data can go from the EU to Japan, but the EU will not allow it to leave Japan to go to the other countries that are part of the CBPR framework. That strength of feeling was true and remains true for the APEC CBPRs.

The question now being asked of those jurisdictions that are inside the tent of the global CBPR framework is, "What is going to be done to address the perceived and/or actual deficiencies that exist in the framework that might reassure the European Commission and help scale the programme?" I believe there is a lot of work that is happening to do that.

It operates very differently to adequacy. First, it is multilateral. Secondly, it is almost an industry-led certification programme. It is not Government-to-Government assessments of one another's standards. It is industry organisations putting themselves forward and saying, "We adhere to the laws of the land in the participating jurisdictions. We have a

badge and a stamp from a trusted third-party agent to attest to that. As a consequence of that attestation, we can transfer data in all of these jurisdictions". It is quite a different model. It does not, therefore, attract the politics and realpolitik that comes with adequacy. "We are assessing you. Ideally, we should converge closer to one another".

That said, I do think it is viewed with reticence by some. Others in organisations and in industry have a lot of optimism about where it might go.

Q15 **Baroness Hayter of Kentish Town:** I left a question hanging on the civil justice side. Do you have any experience of that that you wanted to feed to the Committee afterwards? When we were doing this some time ago, it was not just criminal law. In family law, there is access to children, maintenance, attachment of earnings and an enormous number of privacy issues. It would be interesting to know how any change to adequacy would affect that. I hear we have gone back into Hague now. I am not on top of it any more. If you would like to submit something, we would probably welcome that.

My question really goes back to something that was said right at the beginning by Eleonor Duhs about our adequacy having constraints. What are the implications, constraints or whatever from our new CPTPP membership for any changes or potential changes in adequacy? Even within CPTPP there are other things going on, such as Singapore Digital. I am not quite sure how all of this fits together. What implication would any changes to adequacy have on what we are trying to do globally?

Eleonor Duhs: I am not an expert on CPTPP, but it is problematic. The UK is potentially signing up to different standards that do not necessarily conform to what the EU requires in terms of essential equivalence. That does seem somewhat problematic to me. I am sure Joe has a much more detailed answer than I do.

The Chair: Could we have a fairly brief one, if you do not mind?

Joe Jones: Once upon a time, international trade law was niche. I am glad it is having its moment. It is an imperfect analogy, but I use the analogy of pipes and taps in plumbing. Trade agreements relate to market access. They relate to the plumbing that exists. The CPTPP arrangement and other international trade agreements do not ever turn the taps on. They do not ever permit the free flow of personal data. The taps are the preserve of our data protection frameworks. Adequacy is one such tap; the contracts are others.

CPTPP and other international agreements relate to market access and conditions, data localisation, data storage and entry to the market. Those provisions always accept the domestic regulatory environment relating to the protection of personal data. If we sign up to CPTPP, that does not mean all those countries in the arrangement are adequate. It might put some mood music pressure for that to be the case—you have the pipes, so you could turn on the taps—but it does not result in that happening.

Q16 **Baroness Nicholson of Winterbourne:** I have a very quick request for a point of view rather than knowledge, of which you have already given us a huge and wonderful amount.

On personal data protection, a very good example was when Baroness Ludford mentioned the National Health Service's attempt at merging. The first thing that went out of the window was personal data protection. There were all these trusted partners, of which there were an unconscionable number and none of them were trustworthy in any sense.

Is personal data protection going to fade away? It has already been disseminated and fragmented. It is very hard to get personal data protection in anything now, whereas 25 years ago it was really cock of the walk. It was the top thing. All files were kept separately, as you will remember very well. The merging did not protect the individual files. It pushed everything together. Everything has got considerably more like that, as some of your comments this afternoon have displayed.

Do you see any way in which we can push personal data protection, which matters a lot in the UK with common law, back up a little bit in this line of what is going on? Or is it going to be, in the end, nothing but a few words? Is it going to exist at all?

The Chair: What are your reflections on that?

Joe Jones: When framed as personal data protection, eyes might glaze over in certain circles. When framed as a question of the social contract that consumers have with organisations and their reasonable expectations as to how their information might be used, misused or abused, that is top of register for many individuals. We have data from various surveys to prove this. Consumers move with their feet, increasingly. They change their behaviours. They have a sense of what their information is worth to them, even if they do not have a sense of what that information might be worth to the organisation.

There is that phrase: trust arrives on foot and leaves on horseback. When organisations go through data breaches, many individuals will choose not to do business with that organisation or may go elsewhere. So I do think it is top of register when framed slightly differently.

GDPR and data protection invite technical or esoteric, eye-glazing moments in certain circles. But, at the top, as I mentioned in my opening remarks, these issues have got to the desks of heads of state. They are matters of high politics and geopolitics. We are talking about where data should flow amongst friends and allies and where data should not go amongst adversaries and threats. Everyone has become a lot more hawkish about these issues in a commercial, transactional sense and in a foreign policy and defence context.

Eleonor Duhs: It is absolutely crucial. In the age of AI, machines are going to be making decisions about us in ways that are not transparent. That is extremely dangerous. The rights that are conferred by data protection law are crucial to ensuring that AI is deployed and used in our society in a way that does not exacerbate inequalities and discrimination.

In my firm we are seeing a huge and systematic use of AI to make decisions about workers in the gig economy, including hiring and firing. If we do not take this seriously and come up with the right solutions, that is going to be very detrimental.

The Chair: Thank you very much indeed. That is a very good note to finish on. We are really grateful for your time and your expertise. You have taken us deeply into the subject. The more we learn about it, the more we realise what a deep subject it is. You have brought it to life for us as well. Many, many thanks. With that, I close this public evidence session.