HOUSE OF LORDS

European Affairs Committee

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

Tuesday 16 April 2024

4.20 pm

Watch the meeting

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

Evidence Session No. 2 Heard in Public Questions 17 - 27

Witnesses

I: Bojana Bellamy, President of Andrews Kurth LLP's Centre for Informational Policy Leadership; Zach Meyers, Assistant Director, Centre for European Reform; Neil Ross, Associate Director for Policy, techUK.

USE OF THE TRANSCRIPT

1. This is an uncorrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

2. Any public use of, or reference to, the contents should make clear that neither Members nor witnesses have had the opportunity to correct the record. If in doubt as to the propriety of using the transcript, please contact the Clerk of the Committee.

3. Members and witnesses are asked to send corrections to the Clerk of the Committee within 14 days of receipt.

Examination of witnesses

Bojana Bellamy, Zach Meyers and Neil Ross.

Q17 **The Chair:** Good afternoon, and welcome to the House of Lords European Affairs Committee. We are continuing our inquiry into data adequacy and the implications of that for UK-EU relations. We have three extremely well-qualified witnesses to talk to us today. A warm welcome to everyone.

This session is being broadcast. We will make sure that you have a transcript to correct, and please let us have back in due course. We aim to finish within an hour if we can. I appeal to everyone to keep questions and answers concise, and not every witness should feel that they have to answer every question.

I will ask each of you to introduce yourselves, because you can do it better than I could, and then to say something about the overall existing adequacy arrangements that underpin the data flows between the UK and the EU and your assessment of how things are working at the moment, before we come on to the issues of how they might change.

Bojana Bellamy: Good afternoon, everybody. I am the president of the Centre for Information Policy Leadership. We are a global privacy and data policy think and do tank. We operate out of London, Washington, and Brussels. I am delighted to be here. Thank you very much for this opportunity. It is important that you are doing proper scrutiny of this topic.

I work with lots of global companies but also with other Governments and policy and law makers, and adequacy is a topic that is on everybody's mind. Of course, for companies, international data flow compliance is one of the top three compliance challenges and tasks. Companies are spending probably an unnecessary amount of time on ensuring legal compliance with international data flow provisions, which are quite complex under the GDPR and international regimes.

There is no doubt, in my opinion and in the opinion of many organisations, that adequacy is helpful and should be retained. The way it has been framed today is working very well, because there is legal certainty and the compliance burden of having to legitimise every single data flow from a global or UK organisation, an SME or a start-up will be much less. Today, the regime is quite complex. Companies have to go through a transfer risk assessment for each transfer; they have to go through the legal papering, as we call it, of each data transfer to see whether there is adequacy. If there is not, they have to put in place standard contractual clauses, and if that does not work, perhaps binding corporate rules for the large group of companies, and maybe then for derogations. That is a really complicated process and one that requires quite a lot of resources. It is certainly not something that SMEs, and companies that want to be agile and transfer data and take advantage of global data flows, can do.

There is no doubt that adequacy is a shortcut from all of that, and it is helpful. Of course, adequacy is also a political decision. I have to say that. It is an attempt to expand the Brussels effect globally, and it has been quite successful but not as proven perhaps, as the data proves. Today, we have only 15 adequacy decisions for countries outside the EU, eleven of which were done before the GDPR. Among those countries are Canada, Switzerland, New Zealand and Israel. The others are smaller—the Channel Islands, for example. Then we have four new countries; the UK is one of them, as well as the US under the data protection framework, and, importantly, Korea and Japan.

We have had data protection laws for many years, so why are such a small number of countries declared adequate by the EU? If we could rewrite the laws, maybe we would have done it differently. I think I would have done it differently, but we are where we are now and we have to deal with a concept that perhaps is not quite appropriate for today's world.

I want to make a point on the importance of data flows. It is something that I very passionately believe in, and we have seen the importance of data flows in every survey done by the likes of McKinsey in its 2016, 2019 and 2022 surveys. They talk about data flow surpassing the flow of goods and services. That is incredible. They talk about the importance of data flows not just for large multinationals but for individuals, people like us who are using global services, SMEs that for the first time are able to reach the world, and start-ups. Eighty per cent of start-ups are born global. They depend on global technology, cloud computing, IT technology, even talent from abroad, so it is essential that we as a country enable free and responsible data flows with trust. We have to do whatever is possible to ensure that. I am happy to delve into that more later.

The Chair: Yes. We will unpack a lot of those issues. Thank you.

Zach Meyers: I am assistant director at the think tank the Centre for European Reform. We focus on all aspects of EU policy but with a particular emphasis on UK-EU relations, and my particular research focuses on digital technology regulation. Prior to being at the CER, I spent about 10 years as a technology lawyer in Australia, the US and the UK.

I echo all the points that Bojana just made, in particular that data flows are absolutely essential to any country that wants to have a thriving digital economy. They are essential for everything from communication services to cloud computing, which boosts productivity, and they are increasingly embedded in everyday transfers of trade in services but also trade in goods.

In particular, the UK-EU data adequacy arrangement is critical, because about 45% of the UK's ICT exports go to the EU. I will set the scene by saying that some of the risks are around the loss of adequacy, which have increased significantly over the last few years. That is largely

because of the Schrems II decision, which I am sure has come up in evidence already. Essentially, that decision implied that without adequacy most firms would be reliant on standard contractual clauses (SCCs). I think about 94% of firms use those where adequacy is not available. The Schrems II judgment suggested that in a best-case scenario you would not be able to rely simply on changing your contracts and putting in protections, but that every firm that wants to rely on them also needs to do an impact assessment about how well the data would be protected in practice.

In a worst-case scenario, we are looking at a situation where SCCs (standard contractual clauses) cannot be used at all, because the European Court of Justice in the Schrems II case was very focused on the risk of government access to personal data in circumstances that would not have the safeguards that should apply in the EU under GDPR. Of course, government access to data cannot be protected against through a contract between two private companies, so the loss of adequacy, if that were to happen, would be quite detrimental, much more so than we might have thought five or six years ago.

The Chair: We will come back to that in more detail as we go.

Zach Meyers: Can I provide just a little bit of good news? Compared to a few years ago, when I thought that the stability of the data adequacy arrangement between the UK and the EU was questionable, I think that things have become a lot more certain now, for a couple of reasons. First, when the EU in its decision found that the UK provided an adequate level of protection, the Commission was quite keen to make that decision. There were many reasons why the Commission could have justified not granting adequacy, looking at things like mass surveillance in the UK and bulk data collection. When you read the Commission's adequacy decision, it is quite clear that it is not very interested in delving into the detail of that. It understood that loss of adequacy would have had costs to the UK and to the EU, so it was in no one's interest to disturb that, if possible.

The second factor is that the relationship between the UK and the EU has become much warmer and more constructive compared to a few years ago. That makes it less likely that the Commission will be interested in upsetting adequacy.

Thirdly, as I have written in publications in the past, if there was too much emphasis on data collection and national security access to data, it would show up as a bit of a double standard between the practices of EU member states, which might be deemed not to comply with EU fundamental rights but that do not then block the flow of data between EU member states. In the situation that the UK is now in—not being a member of the European Union—at least in theory, and indeed in practice, if the ECJ gets to decide on it not complying with the EU fundamental rights standards, that could lead to a loss of data adequacy.

The fourth point echoes a point Bojana made about the Brussels effect. The EU is quite keen to use its laws to encourage other countries to meet the same standards. There is some evidence that the Commission has been a bit worried that if adequacy becomes such a high standard to meet that it is nearly impossible for other countries to meet it, in practice countries will give up on meeting EU standards entirely, which would boost some of the other networks of data flows that are less protective of fundamental rights.

The Chair: Thank you. Neil, to round off the introductions.

Neil Ross: Thank you for the invitation. I am the associate director for policy at techUK. We are a trade association and we represent over 1,000 technology companies that operate in the UK. I started my job in techUK doing UK-EU Brexit trade discussions, so I have been at the sharp end of this for five years or so. My colleagues have given you a lot of the atmospherics, but I can explain some of the practicalities of what the adequacy decision means for tech companies and for any company operating in the UK.

The adequacy decision is basically one core pillar of two that make up the UK's free trade agreement for digital services with the European Union. You have the data adequacy agreement, but you also have the digital trade chapter in the Trade and Cooperation Agreement. The two in combination mean that any company that wants to exchange personal data with the European Union as part of its business services just has to comply with the UK data protection law, and that means that they can exchange in free trade with no barriers and no discrimination. That is effectively what these two pillars do to provide massive certainty to UK companies.

Where do we think the state of the adequacy decision is now? I agree with my colleagues that after it was agreed the relationship looked a bit tense, but because the relationship has improved, because the reforms that the UK is planning to put in place through the Data Protection and Digital Information Bill have been well consulted with the European Commission, and the fact that the UK is now planning to operate within this broad framework, the risk of losing data adequacy is quite low.

There are some other external factors that could affect that—the Investigatory Powers (Amendment) Bill, the European Convention on Human Rights, and what the European Court of Justice does in relation to the decision—but it is about as stable as you can hope for. Broadly, we think that we are in a good place and that, when the renewal comes up, we should get through it reasonably okay.

Q18 **Lord Stirrup:** To complete the process of setting the baseline, can you say something about the track record to date of the GDPR and the Data Protection Act 2018? How have they been working in practice, particularly from the perspective of companies and businesses? Where have they been good, where have they been a drag, where have they been

imposing costs in particular? Perhaps Bojana Bellamy might like to address that, and then have any dissenting views or addenda from the other two witnesses.

Bojana Bellamy: We at CIPL have just prepared a final draft of a paper on GDPR at five years old. I am happy to review it with you and give you a preview, but we will publish it in a few weeks' time. We have looked at our own research and evidence and discussed with a number of chief privacy officers and lawyers what we have seen in the last six years, so let me start with some positive impacts.

I think it is important to acknowledge that there is much greater data protection, privacy awareness and ownership in organisations since the GDPR. It has become more of a board-level issue. Companies are realising that this is important not just because this is a law and they will get fined if they do not comply, but because it is part of the overall data strategy of companies that are all about how they utilise data as much as possible but in a responsible way and in compliance with the law. I think the more enlightened companies are realising the link between good privacy compliance and enabling more data-driven innovation products, services and so on. I think that is a very good development.

Secondly, we have seen more investment in privacy management programmes. Certainly large organisations and many UK plcs are not only employing privacy officers but reporting to the boards and audit committees and implementing policies, procedures, rules, tools and training to ensure that this becomes part of the DNA of a company as the company operates. With that, we have also seen improved data hygiene and data management. Companies know where their data is, where it is going, who is touching it. They keep it more secure and there are potentially fewer breaches, but also, of course, more awareness of the need to protect data and perhaps more awareness of when the breach happens. I think it is also true to say that we have seen better awareness among the general public of individual rights. People exercise their right to access objection, their right to be forgotten or their right to deletion in respect of their data.

Finally, the data protection authorities have also stepped up. They are more effective, robust and capable, and they have the technical capabilities. They are doing some innovative things such as regulatory sandboxes. We have seen particularly the Information Commissioner's Office really leading this pack vis-à-vis counterparts in Europe.

There are challenges—

The Chair: I am afraid we have to now go to vote, so I will suspend the session and hope we will be back on air in about 10 minutes.

The committee suspended for a Division in the House.

The Chair: The European Affairs Committee is back after a vote and we have about 30 more minutes with our witnesses, which we will use to

best effect. Bojana, please briefly wrap up what you were saying.

Bojana Bellamy: I will talk very briefly about some of the challenges that we identified in GDPR implementation. There has not been enough stress on accountability and risk-based approach. The risk-based approach of the GDPR is very much enshrined there. It means that you are supposed to implement the rules based on risks and harms to individuals or society, but it has not really been fulfilled, which is a great shame.

There are some other unrealised provisions, such as certifications and codes of conduct, that have not been done. There is a group of substantive rules that I fear data protection authorities have been very conservative about in their interpretation. Their point of view is that data is bad. But, actually, data is good. We have to ensure use of data but in an appropriate and responsible way, but data protection authorities in Europe tend to have the conservative approach whereby less data is better and therefore the legal basis for processing, such as legitimate interests, have been reduced and consent has been boosted, which of course leads to consent fatigue and anonymisation has all but been forgotten. Data flows, which we talk about here, have become very complex, particularly for SMEs. There is also a lack of harmonisation, which is perhaps less important for UK now but is important for Europe.

GDPR is not fully technology-neutral or future-proofed, as we have seen with AI Advent. There are serious tensions in how data protection principles apply to AI technologies. I am glad that the UK Government are taking a different approach to a regulation of AI, because we are more flexible in how we can evolve the interpretation of these rules. Similarly to blockchain biometrics, these are really complicated areas, and I am not sure that GDPR is quite technology-neutral enough for that.

My final point is that data protection authorities have been under huge pressure to show their teeth and to favour enforcement versus engagement, and I am not sure that that creates best outcomes in the market. I think that engagement and proactive incentivisation of accountable practices achieve better results than just enforcement, because companies absorb the cost of enforcement and do not change anything. They have perhaps spent too much time on complaints handling and breach notification, because they are not able to triage in the way we are perhaps able to in the UK. I will stop there, but I am happy to add that.

Neil Ross: To build on the comments that have been made, like with any piece of legislation—if you had passed, say, a criminal justice Bill—you would look back on it in five years' time and ask how it is working, what the real world effects are and how we change things going forward to account for new social or technological developments. The GDPR is very similar. Bojana has highlighted a number of areas where the Bill raised awareness among businesses, public bodies and so on about data that is being collected and spread the awareness of rights among the public. But

now that we have moved five years on we can see that it is potentially costing quite a lot of money for small businesses, we focus more on enforcement than engagement, and it has a series of problems.

In that scenario, you do a legislative review of the Bill and think about changing how it works in practice. That is effectively where we think the UK has got to with the Data Protection and Digital Information (No. 2) Bill, which despite its launch as a Brexit red-tape deregulation Bill in reality is quite a carefully calibrated evolution of the data protection regime, which basically aims to make things a bit more flexible to update the law for new technology and to make it easier in particular for smaller businesses to comply. This seems like a natural evolution of the law and, therefore, we are in quite a good place.

The UK is leading on this. My colleagues might comment on this further. They might talk, for example, about when the Data Protection and Digital Information Bill is implemented, that might then inform an update to the GDPR in the European Union as well. Those discussions are ongoing.

The Chair: We now move on to the next group of questions.

Q19 **Baroness Anelay of St Johns:** Thank you. All three of you have given us a picture of both the advantages and the challenges in the current system. We have heard that it is perhaps at a high level. Can I take it down to detail from the point of view of businesses? In your view, what changes do you believe businesses wish to see? Coupled with that, what changes to the data regime could reduce the burden on business? I have in mind without going back to the old old of having to rely on individual contractual agreements.

Neil Ross: I can cover that point quite quickly. Under the Data Protection and Digital Information Bill there are a few issues that have been pointed to businesses as being the most significant for them. One is the updating of the research provisions clauses. That basically brings the provisions on research, which are the recitals of the GDPR, on to the face of the Bill to make it super clear how you conduct research and can process data for research. There are changes to the legitimate interest provisions, making certain activities very clearly legitimate interest—for example, preventing crime, safeguarding children and so on. That makes it a lot easier to process data to meet those obligations.

They also make it a lot clearer in relation to other things—transfers within a company are easy to use, for example. There are changes to the international data flows regime. The UK is basically going to keep the same approach that the EU has, granting data adequacy to some countries, but we will avail ourselves of extra legal tools should we want to use them, to transfer data to countries or international organisations that we have used also being compliant. It gives you quite a lot of flexibility as well as maintaining the original approach.

There are some specific things that make it a lot easier for smaller businesses. The first thing, though, is that the design of the DPDI Bill is

quite strange in its legislation. It is designed to be new but also completely interoperable with the EU GDPR. Many of our companies will just continue complying to a global compliance posture where they have to deal with the EU GDPR, data protection regimes across a range of countries. They will be able to continue to do that under the UK regime, but companies that have a big research base or have their operations in the UK or are a much smaller company will be able effectively to avail themselves of privacy management programmes that are simpler to implement than the GDPR version and to take a more proportionate approach to how they manage their data compliance. So it helps to balance those two tensions.

For the tech sector in particular, if you were, say, a company that started in the UK, you could avail yourselves of these more flexible rules, but as you scale you have a regime that is sufficiently similar to the EU's and you can quickly move to a global compliance posture.

Baroness Anelay of St Johns: If there are any other questions, perhaps you might give some more detail on the advantage of changes that have not already been mentioned.

Q20 **Lord Jackson of Peterborough:** You will be familiar with the Oxford Martin School academic study of March 2022 looking at the cost of GDPR. Perversely, it seems from that evidence that there is a disadvantage in the legislation in favour of large tech companies and against SME IT companies, for instance. Do you think that was a function of one-off costs, of increasing compliance costs, between 2018 and 2022, or do you think that the situation has changed? Is there further empirical evidence of how GDPR is landing in terms of costs and benefits?

Bojana Bellamy: There are a number of surveys that look at the costs of GDPR. One has to ask how scientific these are, because we do not have economists in companies whose job is to just monitor the costs of implementation and compliance, but we have some. PwC or the International Association of Privacy Professionals together with EY are talking about the GDPR compliance costs to organisations being more than $1 million for 80% plus and more than $10 million for 40% annually. The members of Fortune 500 companies will spend a combined $7.8 billion, which is $16 million each.

There is another interesting University of Oxford economist talking about an 8% reduction in profit in response to the enforcement of GDPR. Equally, we have done some interesting surveys on the return on investment. If you invest in a privacy programme, you are more likely to get a good return on investment because you are a more trusted company, you will have easier negotiations in contracts and business negotiations, and you are likely to have fewer breaches and to deal with breaches more quickly, so there is also the cost of good compliance and good GDPR.

One has to take all this with a pinch of salt, but there is no doubt that costs are huge. Big companies can absorb these costs, because they have

big teams, big resources, chief privacy officers. Tech companies have up to 1,000 people working in product development and developing products in compliance with data protection rules. SMEs do not have that ability at all. We need to ensure that we can help start-ups, SMEs, lots of them in the AI space, perhaps through the ICO's new innovation service. That is interesting. Regulatory sandboxes again are interesting. We cannot avoid compliance by SMEs if they create high risk, which is why a risk-based approach is important. If you create risks to society and people because of your products and services, you have to do something to mitigate those risks, small or large. That is why we need the risk-based approach to how we manage these rules and enforce them.

Zach Meyers: Looking at it from a top-down perspective is quite interesting too—so not at the level of individual businesses but how these new digital laws, of which quite a number in the EU have been passed recently, are affecting economic growth. I do not think it is quite as straightforward as Bojana's studies suggest; they sometimes suggest that GDPR is an innovation killer. For one thing, the UK has lived with GDPR for a number of years now, and we produce more unicorns, which are more start-ups that are valued above $1 billion, than almost any country other than China and the US—and on some scores India—which are obviously much larger in population than us. It seems that the UK can punch above its weight in innovation and have thriving start-ups while still complying with GDPR. I think a reason for that is that it builds trust and creates certainty. Companies that need to do business across borders might as well comply, and comply from the start, with a rigorous regime that is basically going to guarantee that you will meet data protection standards anywhere.

The other potential impact of GDPR on innovation is not about the creation of start-ups but about how technology is disseminated across the economy. When you look at EU productivity growth over the last couple of years, once you adjust for factors such as the lower number of working hours in the EU versus the US, you find that the EU is doing much better than is most commonly reported. It is obviously true that GDPR has costs, and I am not necessarily saying that it is unleashing innovation, but it is maybe not the innovation killer that it sometimes is portrayed to be. The question is more how we make sure that it is as clear as possible for companies to comply with, especially small ones, so that the competitive impact is—

Lord Jackson of Peterborough: Although I was surprised to see that the German CDU MEP Axel Voss, who is a rapporteur for GDPR, said, "Europe's obsession with data protection is getting in the way of digital innovation". That is quite a surprising comment from him.

Bojana Bellamy: You can see that in discussions on the digital regulation in Europe. There is a digital regulatory tsunami where you have competition rules, online safety rules and data sharing rules, and the health data space is incredibly important. All of this is incredibly important, and GDPR is being quoted all the time as being, "We can't

possibly erode the right to privacy". That is why you have seen some unusual requests for example for opt-outs from the European-held data spaces. It is because of GDPR.

There is a lot of really deep thinking and a little bit of a discussion in Europe. Soul searching is what we want. It is important to absolutely protect fundamental rights, but it is equally important to ensure economic progress, competitiveness of the market in the UK and in Europe, and that people can use data and benefit from the medical research, new products and services.

We at CIPL have done a report on the harms of data localisation—to your point about what the cost would be. We have not measured the cost, but there is no doubt that medical research, scientific research, medicine development but also communications and company operations such as fraud prevention, information security, cybersecurity would not be possible to achieve to the levels we want unless we enable data flow. That is why we need that pragmatism.

Q21 **Baroness Hayter of Kentish Town:** I understand what you are saying from the point of view of business. Do any of the changes that businesses are getting or businesses want have implications for consumers or for exactly those people who rely on the present protections? If we are not careful, we are describing this from only one side.

Neil Ross: Absolutely. The key thing is maintaining high levels of trust in your data protection regime. One of the key things that the new Bill goes to—I think that is what you are talking about—is that it does not remove any of the legal rights that underpin the regime. You can still ask a company what data it holds on you, whether it can delete it, whether it can move it to another place. The Bill also introduces some extra stuff that will help people to operationalise their rights—that is an awkward phrase—to basically exercise their rights better with digital ID provisions, smart data provisions, that will allow them to more securely move between different services and engage with government in a secure way. These kinds of approaches to how you exercise your rights better are probably the route to go down.

Baroness Hayter of Kentish Town: That is assuming that a consumer can do that themselves. I am talking about protections for ordinary people who are never going to do that. Are we risking their protections because of relying on them to ask a company?

Zach Meyers: One question I have is around the use of delegated laws as part of the Bill. They are quite significant in how they can change the scope of the Bill—including, for example, the permitted purposes for using data. It is very important that those get properly scrutinised, because you might not want a situation where consumers, who understandably are not following the progress of every piece of secondary legislation in the UK legal system, find that data can suddenly be used for reasons they would not have expected. They will not know that there are those rights that they can rely on to ask about that.

Q22 **Baroness Blackstone:** Can you tell us as concisely as you possibly can what the EU's view is of the UK's approach to data protection?

Neil Ross: We have engaged a lot with the European Commission on the new Bill that is going through.

Baroness Blackstone: The digital Bill going through at the moment.

Neil Ross: Yes. The European Commission is trying to understand whether it operates within the current adequacy framework that it has set out and whether it provides an essential level of equivalence. We will not know until the European Union reviews the UK's data adequacy decision in 2025, but all the indications are that it will assess the UK as maintaining an essentially equivalent level of data protection to the EU GDPR.

There are three broad concerns that the Commission always pointed to. One was onward transfers—the ability of data from an EU system to escape somewhere else. That has been broadly addressed in the Bill. One was redress—whether you can seek redress for a breach of your rights. That is still very much maintained in the Bill. That was the big question it had for the Americans whenever it was looking at the new adequacy agreement that it struck with them. For the UK, that was never really a problem. The third was the independence of the regulator, which was a concern for quite a long time but has now been addressed by an amendment the Government made to the Bill at Third Reading in the Commons, where they removed the right of the Secretary of State to approve the codes of conduct and they put it back to the Information Commissioner.

Zach Meyers: It also depends on who you ask in the EU. The European Commission's perspective on this will be very different to that of some groups of MEPs who are much more adamant about protecting data protection rights and very defensive about any risks. Similarly, data protection authorities and the European Data Protection Board generally tend to take an approach to changes to the regime that is quite defensive. At the end of the day, the decision about adequacy is very much for the Commission, and to a lesser extent for the member states, and they will take political considerations into account. I spoke a bit about those at the start of my evidence and why I think they tend towards a view that unless the UK did something terribly egregious, adequacy would not be at risk from the Commission voluntarily taking away adequacy.

Bojana Bellamy: There are three detailed provisions that will be looked at, although I think they will pass scrutiny. They are the legitimate interest provisions in the new Bill, the research exemptions and the one on automated decision-making. I believe they provide more effective protection, but that is for a separate discussion.

However, the Commission will be looking at government access to data and the use of data for law enforcement, national security and

intelligence purposes. This is the big elephant in every room in data protection discussions and diplomacy in the world today. I think that is what the Commission will be looking at in particular: whether there has been any erosion of these rights and provisions. It will look particularly at whether there are still provisions for necessity and proportionality of any intervention by the Government to access data, whether safeguards for that access are provided in the law and by the law and, importantly, whether there is independent oversight and redress for individuals against such access requests. I think that will be the most important thing.

Q23 **Lord Jay of Ewelme:** In a way, you have touched on this point. If the Commission actually goes to the European Court of Justice, what factors might the European Court of Justice want to take into account if the legality of the EU-UK adequacy arrangement were challenged by NGOs here or wherever?

Bojana Bellamy: That is very possible. Is it likely or probable? I do not know. As I say, I think it will look very much into the provisions of government access to data and will want to look at the criteria in the Schrems II judgment of essential equivalence, as I mentioned. Remember, they are not absolute equivalent laws. That is not what we are looking for; we are looking for those safeguards.

It will look at the data protection law, the scope, the principles, the rights and the effectiveness of the enforcement and oversight by the Information Commissioner. I do not have any issues with that. It will also look at the wider rule of law. Europe is very strong on rule of law, so the membership of the Council of Europe, adherence to the European Convention on Human Rights, and acceptance of the jurisdiction of the court in Strasbourg and the European Court of Human Rights, all play a part. As you know, there is a bit of tension between the European court and the Strasbourg court, so the European court likes to look at these factors as well.

Neil Ross: I think it depends on the kind of case that is brought. Obviously there are two adequacy decisions as well. You have the adequacy decision under the GDPR and an adequacy decision under the Law Enforcement Directive, so it depends where it comes from. Our general sense is that, for the DPDI Bill, that will broadly be fine, even if a challenge came. This point goes back to the fact that if you struck down the GDPR and the Data Protection and Digital Information Bill's provisions as being non-adequate, it would have a cascade of effects across the world, because no other country would be happy with that standard.

There may be a judgment on the law enforcement provisions. These would still have to be tested and we do not know a huge amount about them yet, but Clause 2, I think, of the Investigatory Powers (Amendment) Bill basically makes it easier for security services to access data that is defined as low or no risk to privacy, and it is up to the security services to define that. That could become the feature of a challenge, but, ultimately, if these challenges happen, the UK

Government can amend the law to address them and then we can move on. I think there would be a strong incentive for that, because if the adequacy agreement under the Law Enforcement Directive was struck down, it would also take out a large chunk of the Trade and Cooperation Agreement that is drawn up between the UK and the EU. I expect that if there were judicial challenge, the Government would probably just step in to correct the issue, because the consequences would be so significant.

Q24 **Baroness Scott of Needham Market:** If I understood correctly, I think what you are all saying is that as things stand there is not a huge risk of an adverse data adequacy finding, and if one were to come it would come through the court and it would be part of a much bigger picture. In those circumstances, is it worth businesses putting much time and effort into planning for a potential situation in which the UK was found not to be adequate, or would the process of getting there be so protracted that they would in any event have plenty of time to think about what they might need to do?

Zach Meyers: It would depend so much on the content of the judgment. At least, that is the case with Schrems II; it took a very long time for all its consequences, including its application in other analogous cases by data protection authorities, to filter through. This is still happening today. A lot of the cases that fell out of Schrems II are still on the appeals route. I think there would be time, and you would very much hope that there would be time, because the consequences, particularly if it was a worst-case scenario where there really was no possibility of using standard contractual clauses as a back-up replacement, would be dire for both sides.

I suspect that the powers that be would do everything possible to ensure that there was time for an appropriate adjustment. Enforcement, for example, would not take place immediately in relation to other companies that were not parties to the judgment that the ECJ handed down.

Bojana Bellamy: It would be detrimental to European businesses if there were to be a finding of lack of adequacy, because they would have to go through all these processes of paperology and legal papering data flows to the UK. If you speak to the likes of SAP, BNP Paribas, Accord, big players, telefónicas, German companies, the automotive industry, none of them really want that. It is not in their interests either. I think it is possible but highly improbable.

The Chair: Was that not true in the case of Schrems?

Bojana Bellamy: It was. That is a very good point. I do not think European businesses were very vocal. and I think they regretted that, but you are right: the European Court of Justice has its own mind and it will make a decision based on—

Neil Ross: I think the Schrems II case is quite instructive. I have worked on Brexit for an incredibly long time, and they are still in the same bucket. If there is a big problem that the two political sides can agree

they want to resolve, they will find a way of fudging the boundaries to make it work until a legal solution can be found. I think that would be particularly the case in this instance, because since leaving the European Union the exchange of data to support the economy has grown significantly. For example, you have constant exchanges of data at border posts as you cross between one area and the other. You have to do much more consignment, more exchanges of data. I remember from the process when we were negotiating the adequacy decision that the effect on Ireland was enormous, potentially because of the exchange of data that crosses borders there. So I expect, given the generally friendly relationship that we have at the moment, that you would find a solution to get around it before coming up with an alternative.

Zach Meyers: I think there was a case involving the company Meta that would basically have to have stopped data flows to and from the US, which would have made it impossible for it to provide services such as Facebook. The timing of the EU-US data privacy framework was clearly designed, including with very high-level pressure from the Commission President and the US President, to get that deal done in time so that these data flows did not have to stop. I am certain that if that happened with the EU-UK adequacy arrangement there would be enough political will to solve the problem, although obviously that is not a situation that businesses want to be in.

Q25 **Baroness Lawlor:** You mentioned that not all countries want to join the European Union's GDPR system. Can you explain to the committee how they conduct digital trade, how they approach digital transfers with the EU, and what the main features are of these countries in protecting consumer privacy and digital transfers? I would also like to find out more about individual cases. Can we learn anything about it? We recently signed treaties with New Zealand and Australia, and there, as far as I can see, the digital trade chapters enable the free flow of data across borders, prohibit data localisation and have innovatory chapters.

Could you comment on all three and how they approach the European Union's requirements, what their principal features are and whether there lessons for the UK, including one example—Australia and New Zealand—which we have been involved in, and perhaps others?

Neil Ross: If you are a third country that wants to exchange data with the European Union, you have broadly three approaches. One is that you can find an adequacy agreement, but some countries simply choose not to do that because they do not want to align so closely to the GDPR. Their reasons are probably that in their part of the world they find their digital trade agreements work better with their near countries. Singapore and the US take a very different approach.

That does not really work for the UK just because of where we are geographically and the levels of trade, but you might not choose to have an adequacy agreement. You can then do it through binding corporate roles or standard contractual clauses, but those tend to be for individual business uses or for a group basically to move its data. It is much less

efficient than an adequacy agreement, but it might suit you better because of where you are in the world and the trade you use.

The things that we could learn from those countries is that they often take very flexible approaches to how they think about transferring data around the world. They will do it on a contractual clause basis. They may join multilateral fora or sign up to big contractual ideas like the CBPR forum to give companies more options to exchange data in different ways. The UK is already pursuing all those within our envelope.

The other things that we can do—coming to the Australia and New Zealand examples—are setting up things like tech bridges, shared sandboxes, and all these things you can do while still having an adequacy agreement. It just gives businesses way more options. That is something that the UK can do as an independent country, because you are just more fleet of foot; you do not have to negotiate with 27 countries. In some ways, you can describe the UK as having an EU system-plus. We have taken the one that we inherited, but we have found ways to improve it and grant more flexibility so that we can give businesses and organisations here more options.

Baroness Lawlor: Would you say that it is more conducive to small businesses, given the huge compliance cost and the fact that we try to encourage challengers and entrepreneurs in this country, which is not necessarily the practice with the big conglomerates in the European Union?

Neil Ross: I can definitely say that the shared sandboxes and the tech bridges have really helped smaller companies. They are particularly tailored to companies that want to export to particular markets. I do not have the figures to hand, but I will send our views on those in writing to the committee.

Bojana Bellamy: There are only 15 adequacy determinations done by the EU, and there are 120 countries that have privacy laws. That is why I say that maybe the system is outdated. We drew up these rules when there were no data privacy laws. We were worried about exporting data to safe havens where perhaps our rights could be abused and the rules avoided, but in today's world where we have privacy rules we need some different systems in place other than adequacy. It is interesting in an international arena to hear Kenya saying, "We need to be at the table as well" when it comes to international data transfers. Argentina said, "Yes, we're following GDPR. We're adequate, but we are also looking to Cross-Border Privacy Rules", as do many Asian countries.

Not everybody is copying GDPR because they cannot. They are not at a level where they can copy. They do not have the same philosophy, the same culture, the same economic aspirations, dare I say. It really is not the same. Some African countries are very keen to bring their population and economies to the levels of the western world. We need to be very

understanding of the different needs of countries and not always exporting what we think is the particular way to deal with this.

The Cross-Border Privacy Rules System—Neil Ross mentioned these—is an interesting alternative model to the European model. It started in APEC; hence it is a little more flexible. It is based on accountability, which means that the accountability and protections flow with data. It does not matter where data goes but you, as an exporting entity, have to ensure that data will be protected through all kinds of means wherever it goes. It is based on certifications. Lots of SMEs in Asia are certifying as well, and the UK is now an associate member. Twenty countries were present for the first time in London last year when the CBPR (Cross-Border Privacy Rules) forum held its meeting. This is a thing that we would like to see grow and be upgraded, and raise it to the level of GDPR so that we can create bridges.

I would like to ask for your help to push the Governments of the UK, future and current, to take this UK soft power, this diplomatic power, and the strength of the UK to convene and discuss these data flow issues. This is so important for everybody. We are not having enough discussions about why data flows are good for all of us, why we need data for responsible AI. We would like the UK to have more influence and more leadership in the global arena on this important topic.

I see some of that happening. I was part of the UK expert council on data flows and we issued a report. There are some really interesting recommendations and I am happy to send that for your attention. We want this to be implemented and for the UK to wield its know-how on this topic, because I believe we know more than perhaps others do.

Zach Meyers: I will be slightly more cautious about the enduring impact of the Brussels effect. Of course the number of countries—15—is relatively small, but they are largely democracies that respect the rule of law. We have countries such as Australia that are now revising their privacy laws and are likely to bring their laws much closer to the GDPR over time. There are alternatives, such as the US-led Cross-Border Privacy Rules (CBPR), which are attempting to create a network to compete with the GDPR. I am quite cautious about those. I think there are only 74 firms, not countries but companies, that have signed on to the CBPR. It has quite a long way to go before it can compete with the GDPR in the number of firms that fall under its rules.

The other point to note is that some countries such as Japan and Korea that are signed up to the CBPR (Cross-Border Privacy Rules) but also have EU data adequacy. This has led to the Commission being quite worried about the impact on onward transfers, because the CBPR for onward transfers are not nearly as stringent as requiring data adequacy. So the Commission has tailored the adequacy arrangement for Japan to protect against data flows outside of Japan that would not meet GDPR standards. That means that if firms want to combine different datasets, some with EU nationals and for other nationals, they are managing two

different competing data protection standards at the same time, and that can get quite complex.

The other point I would note is that the CBPR was led by the US, and the US position on free flows of data seems quite confusing. I am not quite sure where it is now. It withdrew its support in the WTO recently for principles that would promote the free flow of data for e-commerce on the basis that it wanted to preserve its right to better regulate data protection within the US. I think that poses a bit of a question mark on where US leadership is on this, because they were the real promoters of the CBPR. Bojana might know some more about this, but it seemed like an odd decision by the US to me.

Bojana Bellamy: If we can disagree here, I perhaps do not share your view, Zach, on CBPR (Cross-Border Privacy Rules) potential. I think it has lots of potential. The US is still pushing, but not just the US; Japan, Korea and Singapore are also pushing, and the UK is an associate member now. There are, as I say, a number of countries that are looking at this. It is still quite compatible with the recent US Executive order. We have to understand that countries have concerns about their data sovereignty and digital sovereignty from time to time, particularly in respect of data flows not to like-minded countries perhaps but to non-democracies. It is very difficult, and I do not want to put any countries in one or the other camp, but that is to be expected. That still does not preclude a country being careful about data and digital sovereignty and participating in data free flows with trust.

I think that there is a momentum. CBPR has a momentum because it is becoming global. It is leaving the APEC source where it started. The OECD trusted government access to data principles are an important international commitment. The UK played a very important role there, and I would love to see now what the Government can do to publish how we comply with these principles. The more we and everybody else publish how they use their data for national security intelligence purposes in compliance with the OECD principles, the more trust there will be for this data free flow with trust initiative. That is a G7, G20 initiative, again involving not just the US but Canada and Japan—big economies, including our European friends, France and Germany. Germany is also observing the CBPR (Cross-Border Privacy Rules) discussion.

I feel that we are in a good place and there is a momentum gathering for perhaps a new deal on data, but we need some leadership in international fora to build on what we have, pull all the strings together and discuss this with like-minded countries first.

The Chair: We love it when our witnesses disagree. I just want to give the floor briefly to two colleagues who have not yet spoken, Baroness Nicholson and Baroness Ashton.

Q26 **Baroness Nicholson of Winterbourne:** Many of the countries that you have mentioned in the last few minutes simply do not share common

standards with the UK in looking after their citizens' rights. It is enormously important to listen to countries that have had a particularly difficult past. Germany, for example, is unhappy about our current Bill going through Parliament. Of course, one of the German cities was the very first data protection creator immediately after the Second World War. It came from there. We have been following those common standards in different ways in conjunction with the EU all the way through. It is very important that we should listen to what the Germans have to say. Somebody was laughing about it earlier, but that is not the case. They have learned the very hard way about dissolution and endless sending of citizens' data around. Look what it did to them.

I suggest that although it is lovely to be leaders—I am a former computer person myself, and nothing is more fun than coming out in front and leading on this—none the less our job here in Parliament is to consider the citizens' rights. It is very important indeed that we do not forget that which is in danger of being forgotten in these very merry discussions about how we are going to lead on data protection. That will not be data protection; that will be data dissemination.

Q27 **Baroness Ashton of Upholland:** Baroness Nicholson makes a good point about how GDPR arose in the EU and the combination of countries and histories that formed the backdrop to feelings about protection as well as about markets and innovation and so on. One is always mindful that, if you pull together a group of countries, that will happen, and it will happen in any grouping in any event. However, while we have the GDPR certainty—I am heartened by what you are saying about that and the fact that our trade flows mean it remains a cornerstone of what we need to do—it is important to innovate as well. I think that is the point you make. I am interested in any very brief words you have on what you see could be the process of evolution of GDPR, not a big bang from one to the other, if you take these two competing ideas of certainty and GDPR based on culture, history and need and the innovation that could come from countries that are thinking slightly differently. Where do you see the innovation?

Baroness Nicholson of Winterbourne: Does the point you are making not also rest on trust, as you mentioned a number of times? Of course, the general public do not have trust in these systems, and quite rightly when you see how data flows emerge all over the globe. There was another huge leak of data this morning. It was more than a leak, actually, meaning that personal data has gone everywhere. Nobody knows where it is, so do you not think that should also be built in at this stage when you are going to change?

The Chair: Perhaps we could wrap up with comments from each of you on those very important points.

Zach Meyers: As we said earlier, what we need is not revolution but evolution, and as part of that I see an ongoing dialogue between the UK and the EU being very important. The EU is about to do a review of the GDPR, and there may be some reluctance to reopen it. It will be highly

lobbied from all sorts of interest groups pursuing their own ideas. There is no guarantee that what you end up with after the complex EU lawmaking process will be better than what we started with, but I think the UK has the potential to test some ideas.

In a lot of cases, the UK is proposing simply to return to what GDPR was supposed to do in the first place. It was a risk-based proportionate approach to data protection whereby companies that are doing more high-risk activities need to spend more money and do more to ensure that citizens' rights are being protected. Risks that are more theoretical, or where there is a legal risk on paper but which in practice does not seem to have occurred over many years, which is the case with some of the risks around cross-border data transfers, may not need quite as much protection as GDPR currently insists on.

The ability for the EU to adapt to this will be made somewhat more difficult by the fact that the ECJ now sees GDPR as the embodiment of EU fundamental rights that are set out in the EU treaties and in the EU Convention on Human Rights, and I worry that that limits the EU's flexibility a bit. I nevertheless hope that we see this as part of building trust between the UK and the EU at a political level, as well as ensuring that there is continued trust between consumers and companies. I hope that we see this as a dialogue and that we continue to engage with the Commission and other EU stakeholders on the direction of travel and why we think the the UK's GDPR reform is a good idea.

Neil Ross: We are six years into the GDPR process, because it was leveraged in 2014-15 and implemented in 2018. This feels like the right point to sit back and review how it has gone, and the UK Government have attempted to do this in the Data Protection and Digital Information Bill. From our own experience at techUK when we came to consider the question of how important data adequacy is in alignment with GDPR, when it came to the Brexit negotiations, it was our number one ask. Maintaining that same level of rights and responsibilities was seen as absolutely key, not just because it is a global standard but because it was also seen as a signal that the UK was not going to significantly deregulate in this area.

When it came to how we should reform the data protection rules, the Government asked a number of questions, such as whether we should start to charge for subject access requests and whether we should get rid of the right to have an automated decision reviewed completely. When we spoke to our members they said that they firmly opposed both of those provisions, because for them it is not just about the ease of sharing and using the data; it is about the fact that consumers have trust in the ability to hand it over to them, to develop and to use their products. That is a permanent balance that we will always end up doing with data protection law.

There are some innovative tools from other countries that you might think about looking at. There is having secure channels to trade between,

say, bloc A that has certain set of rules and values and bloc B, so that you can do that but still have respect for each other's traditions and rights. There are sandboxes that you can develop within countries to look at how to test data in particular ways and certain products. I think we have currently advocated for an online safety sandbox, because we want to see how we can test data products to improve online safety in line with the new regime that is coming out. Fintech has been quite successful in that space, and the ICO has also done privacy enhancing technologies. We are also seeing regulators lean in and say, "How can we work more proactively with you to ensure responsible innovation so that as you build a product we know that it meets our standards and then it can roll out to the wider market?"

That is where we are in this evolution phase. We might come back and look at it all again in six years' time, but I think the correct approach is to do it step by step and cautiously but optimistically to ensure that you get the right balance for businesses and consumers. In our experience, that is what the companies tell us they want us to do and therefore why I am saying it to you.

Bojana Bellamy: One of CIPL's think tank's missions is to enable responsible innovation while protecting fundamental rights. Privacy is one of those fundamental rights. It is not one or the other; we have to have both. There are ways in which we can innovate. Putting more emphasis on organisational accountability and requiring companies to be responsible and accountable to implement privacy management programmes, reporting to the board—senior executive responsibility—which you see in the data protection Bill, is one way forward.

A risk-based approach is important, focusing on areas that potentially will create harms for individuals and where we need to bring individuals, because as we go through this technological revolution nobody is very comfortable with what is happening to all of us, with AI and neurotechnology. What is next? Quantum computing. We need to bring people on this journey, so, through organisational accountability and transparency and with a smart regulator, that is what we all have to do. There is a role for government and education, of course.

Smart regulation is important, and that means principle-based and outcomes-based to stay future-proofed. Do not tell people exactly how to write a privacy notice; tell them what they need to achieve. They need to achieve trust in the market. We need to solve the trust deficit. Do not tell me exactly how many points I should write in a privacy notice, because nobody is going to read that legal notice, but if I am outcomes-based I have to ensure that there is transparency and that people trust me. Then I will do whatever I can—videos, explanations, FAQs. I will tell them what I will not do. That is not required by the law, but it creates more trust than perhaps telling them what I will do that nobody reads.

We have to change a little bit how we think about this. I feel that the UK has that approach to better regulation, an agenda for what smart

regulation looks like, and of course enforcement and oversight by a pragmatic, risk-based, strategic regulator such as the Information Commissioner's Office. I think we have the right ingredients so that we can innovate. Let us hope that the rest of the world will follow.

The Chair: That is a very good note to finish on. Thank you very much. I am glad that we could get through the session. You packed a lot in for us and gave us a lot for us to think about. I am very grateful for all your time. If you have any further thoughts that you would like to send us in writing, we would be very grateful. You might also like to send us the report that you referenced. With that, the session is closed.