HOUSE OF LORDS

# European Affairs Committee

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

Tuesday 21 May 2024

4.15 pm

Watch the meeting

Members present: Lord Ricketts (The Chair); Lady Anelay of St Johns; Baroness Ashton of Upholland; Baroness Blackstone; Lord Jackson of Peterborough; 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. 7 Heard in Public Questions 72 - 79

### Witnesses

I: Professor Peter Swire, Professor of Law and Ethics, Georgia Tech Scheller College of Business; Josh Lee Kok Thong, Managing Director, Asia-Pacific, Future of Privacy Forum.

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

Professor Peter Swire and Josh Lee Kok Thong.

Q72 **The Chair:** Welcome to the House of Lords European Affairs Committee for the continuation of evidence sessions for our inquiry into data adequacy and the implications for UK-EU relations. I am delighted that we have two witnesses today to talk to us about the wider global perspectives on data and privacy. We have Professor Peter Swire here in the Room from Georgia Tech Scheller College of Business and Josh Lee Kok Thong, managing director of the Asia-Pacific Future of Privacy Forum, who is joining us from Seoul—so we thank him very much for staying up very late in the evening for us. We will transcribe this and make sure that witnesses have a copy to correct before it is made public. We will have questions for you both; some of the questions will be more relevant to Peter and some more relevant to Josh, so perhaps people could indicate when there is a question that is more applicable to one witness or the other, that would be great—and we will aim to wrap this up within an hour.

I start with a broad question. You are looking at this issue of the UK and the EU and data adequacy from a global perspective, and you have both had experience in different ways with the European Commission and the EU approach to data adequacy. Could you start with some general reflections on how that looks from your two perspectives in Asia and the US in terms of the EU's approach to data adequacy?

***Professor Peter Swire:*** It is an honour to be here today. I shall try to share what I can with you all on these issues. I shall give a moment of background on myself, because I have been working on these issues longer than most. in 1998, I wrote a book on EU-US data privacy and the coming conflicts about this, which has kept me busy ever since. That was the year that the data protection directive went into effect. In the year after that, I went into the White House as President Clinton's chief counsellor for privacy, in 1999 and 2000. That was the time when we were doing a lot of privacy laws in the United States; we had the HIPAA medical privacy rule, for example. We also negotiated the US-EU safe harbour agreement, and I was the White House privacy official at the time when that was negotiated, so I lived through safe harbour in quite some detail.

I returned to being a professor after that, and the next government service relevant here is when, in 2013, Mr Snowden released quite a lot of information—you have heard about this. In the wake of that, President Obama created a five-person review group to say what should be done with the NSA, and I was one of the five members of that review group. We published our report—including as a book by Princeton University Press—and quite a few of those recommendations were adopted, either by the Administration administratively or through the 2015 intelligence reform law.

Also relevant here is that, in 2016 and 2017, I was a witness in the Schrems II trial—the case in Dublin where Max Schrems was challenging Facebook. I was selected by Facebook but under the rules was considered an independent expert, and Facebook could not talk to me the whole time I was an expert. I say that because I wrote more than 300 pages of testimony explaining the US intelligence system relevant to EU privacy law. There was quite a lot of detail, as you can imagine. I was trying to be a bridge between knowledge of the US system and knowledge of the EU system. I was even a student in Brussels at the Université Libre de Bruxelles one year, back when I was a student.

Coming out of that, in 2018 I formed a think tank, the Cross-Border Data Forum, which seems quite relevant to today's event. We have a fabulous French professor called Theodore Christakis, a former US State Department counsellor in Brussels called Kenneth Propp, a wonderful China expert, and so forth. I am the research director for the CBDF, and a very large part of my research and attention is on how we might proceed here, including working on the issues that are directly relevant to US adequacy and the recent decision by the Commission to grant that.

That is my background. You asked me for my general views on privacy, but I thought that it would provide some context because, for better or worse, I have been around these issues for quite some time.

**The Chair:** We shall come to the individual issues as we go through the discussion, because you are very well placed to comment on them one by one.

***Professor Peter Swire:*** I have three points to make initially about the US Government's perspective over time on these issues. The first is that there is an increasing appreciation over time that the EU and UK get to write privacy laws to govern data about their own people. It is normal that Governments can regulate that in their economy, and it is now something that almost every major country in the world has now. Twenty years ago, the US was not ready for that; now there is a wide appreciation that it is normal for there to be data protection.

Secondly, there is an enormous difference between the position of the Commission and the jurisprudence to date of the Court of Justice of the European Union. The Commission has great expertise and very good lawyers. Bruno Gencarelli leads the office, now that he has been promoted. They have a great amount of sense of these issues and wrote the very long UK opinion. The Court of Justice has had an extremely strong view about the importance of protecting fundamental rights, and the fundamental right that it is most expansively interpreting is on a person's data. Judge von Danwitz wrote the Schrems opinions and will probably write a third one, if there is one, and he has been giving speeches about how central to the project of Europe he thinks the protection of fundamental rights is. That means that, when the Commission says yes, it is not over. It also has to get past the Luxembourg court, and the Luxembourg court has already shown that it

is willing to apply great scrutiny. So among US government officials there is an appreciation of that.

Thirdly, the US Government, in my view, did the best they could to meet the European Union's legal concerns in the data privacy framework. In my view, they went up to the limit of their constitutional authority in various ways. These days, the US Government respect the project of data protection and protecting rights. They have really gone above and beyond to try to meet European legal standards, yet still face the possibility that the new framework will be struck down. I will stop there.

**The Chair:** That is a very good introduction, thank you. Over to you, Josh, for a quick overview before we go into the detail.

***Josh Lee Kok Thong:*** Thank you for the privilege of being able to give evidence before this distinguished committee. It is probably apparent from how I look that I certainly do not share the same depth of experience that Professor Sawyer has. To give some background about myself, I am currently the managing director of the Asia-Pacific office of the Future of Privacy Forum—more on that in just a bit. Prior to this role I served in the Personal Data Protection Commission in Singapore, where I worked on AI governance and regulatory matters. Just before that, I worked in the Ministry of Law as a legal policy officer, working on matters relating to content moderation, health and safety, among other things. It is a privilege to be here.

The Future of Privacy Forum—FPF—is a global non-profit organisation. We have offices in Washington DC, Brussels, Singapore and Kenya. We have a presence in Tel Aviv, as well as in New Delhi. Our mission is simple but very long-term: to advance pragmatic privacy and data protection principles in support of emerging technologies. We also convene stakeholders from industry, government and civil society to build a more trusted data protection ecosystem. In a nutshell, that is what FPF is about.

Regarding our viewpoint on the data adequacy arrangement at present, from a global viewpoint, I will make three points. First, data adequacy is merely one tool in the entire data transfers toolbox of the GDPR. There are also model contractual clauses, verification mechanisms, binding corporate rules and even codes of conduct. These are all part of the toolbox and they can be used by regulators alongside, or in the absence of, adequacy.

The biggest advantage of adequacy over other tools is that any and all transfers of personal data in the adequate jurisdiction can flow unrestricted and without any other formality, legal fees, and so on, to the jurisdiction issuing the adequate status. This is one of the many reasons why the standard for issuing an adequacy decision is high.

Secondly, it is important to keep in mind that the Court of Justice of the EU—CJEU—has been showing increased scrutiny over the past decade; first, when it comes to ensuring an effective overall level of data

protection in the EU, and, secondly, when it comes to transfers of personal data outside the EU to third countries, emphasising the importance of protecting fundamental rights. When the European Commission acts on matters related to data protection, including data transfers, it is helped by the high bar set by the CJEU.

Thirdly, the culture of ensuring a high level of protection for personal data in the EU is to be taken into account when analysing the data transfer regime there. It is also important to understand and acknowledge, with respect, the cultural, historical and legal context of the various jurisdictions around the world in the context of international data transfer. This is particularly relevant when analysing the development of the national data transfer and the regulatory tools between countries in the APAC region and the EU, varying from neutral adequacy decisions such as the EU-Japan decision, to agreed common road maps that compare and align the EU standard contractual clauses and the ASEAN model contractual clauses, as was the one promoted by Singapore's Infocomm Media Development Authority and the European Commission last year.

I will keep to these three points for now. I am happy to take more questions.

Q73 **Baroness Blackstone:** Could you tell the committee about the approaches to data privacy regulation of the US, Japan and Korea, and how far they differ from GDPR?

***Professor Peter Swire:*** I will summarise the US approach in three or four points. First, there is commercial data and there is government access to data. Commercial transfers—a company just doing its business—can be protected either through a law that is adequate or a contract where everybody promises to hold themselves to the high standards. That is solvable. In the US, if a company promises to follow EU- or UK-level standards, it is subject to enforcement as a deceptive trade practice if it breaks its promise. Companies can promise in a contract to do good privacy and they can be enforced against if they break their promise. That is the commercial world; it is relatively straightforward.

The complexity comes with the history of government access to data. The Schrems cases, which we will get to later, were about intelligence access to data. The US has had a long history of protecting privacy against government invasions. The fourth amendment says that you cannot have a search without a warrant. The third amendment, less known, says that you have privacy in your home, and that the Government cannot quarter soldiers in your home except during wartime. That came out of some experience of the 1770s, with certain British soldiers living in some Boston houses. The point is that there is a long history of scepticism towards government intrusions in the US and of protections against them.

in the 1980s and 1990s, and especially after 9/11, the regulatory paths of Europe and the United States shifted. The US might have ended up with a privacy law in 2001 and 2002 because of the internet, but 9/11 happened. When 9/11 happened, all the attention from government was on sharing the data you need to get the terrorists. Someone coming along and saying "Privacy should win" was not going to win as much as 9/11 and the Iraq war did.

The US approach today is of the last 25 years of Silicon Valley innovation and "Go ahead and try new things". That has been the regulatory approach for commercial data. Many people in Congress believe that it is time to pass a law in the United States that looks like, let us say, three-quarters of GDPR, but it has not happened yet. It might happen; I hope it happens. For the commercial side, it is not going to be a huge problem if you just promise to be good. It is the government access side that leads to the problems.

I have one additional point because of things that happened this spring. Congress passed some new laws about data brokers selling data to China, which I wrote about just last week, and it is published on our website. President Biden issued an executive order in late February. The politics of this is easy to understand. There were studies that found out that the Chinese Government could buy data broker data tracking US military personnel around the United States, because you can buy and sell location data, and some of that location data is military. Then, you can buy and sell military location data. Because we do not have an overall privacy law, this is a problem. In my experience, upon being asked "Should China be able to track the military?", any politician will say "No, we really should not be doing that".

Just a few weeks ago, Congress passed a Bill unanimously in the House—hard enough to do—saying that these kinds of sales of data to China and other adversaries such as Russia are illegal. There is a new chapter of the US approach to data privacy. It is talking to Five Eyes partners about this. The new chapter is, "Watch out for national security-sensitive data of our citizens going to adversaries such as China". That is a different thing about adequacy in the EU—it is not the main thing—but it is another way in which national security is coming into these discussions, even around commercial data practices.

***Josh Lee Kok Thong:*** I thank Professor Swire for that introduction regarding the US regime. I am reminded of my classes on information privacy when I was studying at Berkeley Law, so thank you for that masterclass. I will try to emulate his example for Japan and South Korea.

Let me provide the committee with an overview. Japan and South Korea are jurisdictions noted particularly for their maturity, proactiveness and capability in data protection, as well as emerging technology, in the Asia-Pacific region. Relative to the entire APAC region, their data protection frameworks are some of the most robust and share alignment with

international practices, all while maintaining unique characteristics reflective of their cultural, historical and legal backgrounds.

I will just provide some brief context on both of their overall frameworks. Of course, if the committee wishes to learn more about any particular aspect, I would be happy to take more questions or to submit evidence in writing for your reference.

Japan's data protection regime is headlined by the Act on the Protection of Personal Information—APPI. It was first enacted in 2003 and is a comprehensive data protection law that covers personal information related to a living individual. Based on high-level features and academic analysis, the Japanese data protection regime is one that is pro-economy with a focus on business opportunities. It should also be noted that, in Japan, the right to privacy is implicitly, not explicitly, recognised by Article 13 of the Japanese Constitution; this is supported by tort case law.

Commentators have noted that, based on the original APPI, there was almost no possibility of obtaining adequacy from the EU. Some of the reasons include, first, the fact that the original APPI reflected the broader lines of the 1980 OECD privacy guidelines, rather than the more prescriptive EU data protection directive. Secondly, when the APPI was first enacted, there was no unified data protection law—or, rather, no unified data protection regulator. Relevant ministries were applying the APPI to their respective sectors. Thirdly, there was a small enterprise exception so that small businesses handling personal data from 5,000 individuals or fewer did not have to comply with the APPI.

In the context of adequacy, the APPI subsequently underwent significant amendments in 2015, 2020 and 2021 to strengthen data privacy protections. The Japanese Government added elements that aligned more closely with the European framework; for example, the 2015 amendments introduced a set of enforceable rights. They also established an independent supervisory authority in the form of the Personal Information Protection Commission—PPC—to oversee and enforce the APPI. The 2020 amendments clarified the extraterritorial application of the APPI as well as the disclosure and due diligence requirements for cross-border data transfers; they also introduced a mandatory data breach notification scheme, among other things. The 2021 amendments established a unified data protection system for both businesses and administrative entities of central and local governments; they also expanded the scope of an exemption of the APPI for the use of personal information in academic studies, and introduced more detailed regulations.

I will pause there for now and turn to South Korea. Under the constitution of South Korea, rights to privacy, the privacy of communications and freedom of expression are recognised as fundamental rights. That is already a distinct difference between Japan and South Korea. It is just one instance of the diversity that we see in the entire Asia-Pacific region. For South Korea, with regard to its data protection regime, the starting

point is its Personal Information Protection Act—PIPA. It was amended in 2023 but first came out in 2011; this is perhaps a quick introduction to the alphabet soup that will come up throughout the course of this entire hearing.

The PIPA, together with its implementing regulations, regulates collection, use, disclosure and other forms of processing personal information by controllers. South Korea's data protection laws provide very prescriptive, specific requirements throughout the life cycle of the handling of personal data. Under these laws, the data subject's consent is almost always used as the main legal basis to process personal data. South Korea's data protection regime tends to provide prescriptive, specific requirements throughout the life cycle of the processing of personal data. They are known as some of the strictest sets of data protection laws in the world, given these specific requirements around prior notification, obtaining consent and relatively heavy sanctions, as prescribed by law.

South Korea's main data protection regulator is also known as the Personal Information Protection Commission but is abbreviated to the PIPC. Its key roles are to enforce the PIPA; to impose sanctions and fines; and to shape data protection policies. It is a central administration body under the Prime Minister's office as an EU-type data protection authority. It is supported by other agencies, such as the Korea Internet & Security Agency and the Korea Communications Commission.

The PIPA underwent major amendment in 2023, with most of the changes having since taken effect. The legislative purpose of these changes was aimed at ensuring compatibility and interoperability with global regulatory regimes. Some of the key changes included removing different legal regimes for online and offline businesses and expanding the legal basis for cross-border transfers of personal data, including allowing cross-border transfers if the overseas recipient to whom the data is transferred has obtained a data protection certificate that is designated by the PIPC. The amendments also granted the PIPC the authority to suspend a cross-border data transfer if, for example, the transfer is in violation of the PIPA.

That is really just a whistle-stop tour of the regimes currently in force in Japan and South Korea. I will pause there for now.

**The Chair:** Thank you very much indeed. I am looking at the clock—I am going to have to play the usual chairman's role. You have given us a lot of rich background, but now we really need to focus on the operational issues that are relevant to our inquiry into UK-EU data adequacy. If we are going to finish this session in an hour or an hour and a quarter, we will have to be a bit more concise, if you do not mind.

Q74 **Lord Stirrup:** Professor Swire, can we go back to the Schrems judgments? Clearly, they are something that this committee is closely focused on, in case something like that happens with the UK. Can you

help us understand, first, the real impact on US companies and businesses of the Schrems decisions when they were made, before the implementation of the latest data framework? Was it seriously damaging? Was it a nuisance? What was the scale of it?

Secondly, it seems quite likely that we are going to have a Schrems III. You indicated earlier that, in response to Schrems II, the US Congress had gone about as far as it was constitutionally capable of going. Does this mean that, if the Court of Justice issues a judgment on a Schrems III that is unfavourable from the US perspective, that will be the end of it as far as the US and EU arrangements are concerned? How is it possible to have stable data transfer arrangements between businesses if policy formulation—which, as you say, is carried out by the Commission—will always be subject to individual cases brought to the Court of Justice and what seems to be a pretty activist approach by that court?

***Professor Peter Swire:*** I shall try to be concise.

**Lord Stirrup:** Yes. Condense the 300 pages.

***Professor Peter Swire:*** Right. In terms of the impact, the Schrems II judgment cast serious doubt on the lawfulness of many transfers to the US. Companies were supposed to do a transfer impact assessment to see whether the US was good enough. As a lawyer, I would not sign any of those because I did not see a lawful basis for the transfer. Other lawyers found room to sign and to say that it was okay to export the data to the United States—that is, to say that the US had enough protections even after the judgment—but that would have been a hard position to maintain if there was follow-up enforcement. The ban is a real ban. The ban is this: companies cannot protect themselves if they have data and the Government can get the data. It is the Government getting the data that causes the problem. Everyone knew that it was being negotiated but the impact on lawfulness of transfer was enormous.

The second question was about what would happen if it got struck down in Schrems III. My answer is that it depends on which of two ways that goes. One criticism by the court in Schrems II is called redress: there has to be an effective way to fix things for the data subject. The other one is proportionality and necessity. Redress, which is where I spend most of my time, is where the US has gone to great pains to meet the European legal standards. There is no publicly published approach that can fit the US constitution into the EU standards, except the one that has been adopted. With redress, we could be in a real problem in which Europe says these are fundamental rights and the US says that it cannot do it, based on its constitution. That is a constitutional legal crisis.

The position on proportionality is more like, "You need to move a little more this way or a little more that way". There are ways that proportionality could be struck down, so that the US goes back to the negotiating table. However, there are serious consequences if the redress part is struck down, because it is not possible to amend the Charter of

Fundamental Rights or the US Constitution. We would have to play some pretend game and I do not know how that would work.

Q75 **Lord Jackson of Peterborough:** Professor Swire, broadly speaking, what is your view of the US-EU data adequacy decision? For the purposes of the committee, what implications does that agreement have on UK-EU adequacy?

***Professor Peter Swire:*** This carries on from what I was just saying. You mentioned the possibility of calling this court an activist court, and it is hard to predict how far judges will go. My view of the data protection framework is that the US made a good faith effort to meet European legal standards. I know from meeting government officials and the Commission over more than two years that that is the case.

I believe that the redress procedure should survive. That is my view as a lawyer, but I am not a European lawyer and I am not on the Court of Justice.

There is uncertainty about where the court will go. There are compelling stories that would lead the framework to be upheld, but repeated arguments from critics that a court could go with. As a lawyer and a law professor, I believe that it could go either way.

Here is how it is relevant to the UK: when it was a member state of the European Union, the UK did not have its national security activities examined in the same way by the Court of Justice. It did by Strasbourg, and you have had a lot of practice with the Strasbourg court, but not by Luxembourg. Now the UK is a third party and data goes from Europe to the UK, which is outside Europe now. The scrutiny of the court is part of its general jurisdiction to look at commercial data flows, with some ancillary national security stuff. The Court of Justice doctrine is to look full out at the national security and law enforcement actions of the UK. There is no limit under the treaty, as there used to be.

The Court of Justice struck down Canada on a passenger name records case for not being good enough. It struck down Schrems I and Schrems II. To my knowledge, it has never upheld government access from a third state, so we do not know what it takes to get it to say yes.

**Lord Jackson of Peterborough:** But it has been flexible in the US-EU agreement.

***Professor Peter Swire:*** This is the Court of Justice. The Commission has been flexible. The Commission has been good lawyers for the position it is in. They have to tell their court that they are acting in good faith and have it be defensible, but the Commission wants to make things work with good privacy. The Court of Justice has been saying no and no and no. It has not yet said yes to any regime for government access, and the UK regime is subject to possible criticism for that. You have been around the RIP Act far more than I have and there are critics of national security and law enforcement access.

I will mention one other issue on which you may not have focused. The debate about end-to-end encryption may be relevant here. I do not know exactly where the proposal is—I do not think it has been enacted—that requires communications providers to decrypt and not have end-to-end encryption. That is an invasion of privacy compared with having encryption the whole way. It could be its own part of a challenge in the Court of Justice, as one reason that the UK is not protecting privacy enough is that it is insisting on the ability to break the privacy of communications. That is worth considering and exploring, as it has not been discussed as much.

**Lord Jackson of Peterborough:** Finally, has the US Supreme Court opined on any of this as it impacts the fundamental rights of American citizens, as enunciated in the US Constitution?

***Professor Peter Swire:*** The US Supreme Court has 200 years of interpreting probable cause and what is enough protection against government invasions of privacy. The fourth amendment, the Government's search requirements, are quite strict—as a professor, I have written about this—compared with almost every other country. National security laws in the United States have protections that go well beyond any published protections in Europe. The UK has very good protections for redress in its Investigatory Powers Tribunal, from what I can tell, but there are other parts that would be subject to question. Is that responsive?

**Lord Jackson of Peterborough:** Yes, that is helpful.

**Baroness Lawlor:** For clarification, we are really talking here about the problem that arises with the transfer of EU data to the US.

***Professor Peter Swire:*** Or to the UK—yes, that is correct.

**Baroness Lawlor:** We are not talking about data transferred internally, because that is governed by the law.

***Professor Peter Swire:*** We are not talking internally, US to US. For international business or online commerce, the scope of GDPR for jurisdiction is very expansive.

**The Chair:** Are there any other questions for Professor Swire, before we turn to Josh on the Asia-Pacific side? That was comprehensive and quite concerning, and you have put down a number of quite important markers. I think I am right that there is not yet a Schrems III case being brought, but it could always come.

***Professor Peter Swire:*** People expect that it will come, at some point.

Q76 **Baroness Anelay of St Johns:** I shall address these questions to Josh. In answering Baroness Blackstone earlier, you gave us quite a strong overview of the data adequacy methods, in both Japan and South Korea. So I will not ask you to go over that again. However, I will ask you to go

deeper, in saying what changes you consider Japan and South Korea had to make to achieve the adequacy level that would satisfy the EU. I realise that you mentioned several pieces of new legislation in Japan; was that all of it or was there more than that?

***Josh Lee Kok Thong:*** Thank you for the question. I do not want to go over old ground, but it is worth reiterating that there is a significant difference between the EU and Japanese approaches. While the EU considers data protection and privacy to be fundamental rights, the Japanese framework emphasises the importance of data as an economic commodity. With that in mind, we can turn to some of the changes that were made by the Japanese Government in the journey to getting adequacy.

Some of the main changes include a broader definition of sensitive data, greater individual rights, stronger limits on the use of personal data that is provided to third parties, and enhanced enforcement powers for the PPC. It is also worth noting that, during the adequacy negotiations, the EU negotiated further changes with Japan that culminated in a set of supplementary rules that was issued by the PPC. That had the full effect of legislatively enacted law. Some of these ensuing protections, interestingly, apply only to EU-originated personal data.

This essentially creates a dual-track system. There is one track for data originating from Japan, and one track for data originating from Europe. For example, the APPI's list of sensitive data was extended to personal data received from the EU concerning an individual's sex life, sexual orientation or trade union membership. That extends protection for "special care required personal information" under the APPI to categories recognised as special categories of personal data under the GDPR. Discussions led to a further series of commitments by the Japanese Government which were collected in an annexe to the Commission Implementing Decision, and one of these relates to the requirement for periodic reviews of the adequacy finding.

The journey for South Korea's adequacy data appears to be less known, but I am aware of at least three issues at play. First, while South Korea had initially proposed the scope of an adequacy decision only to parts of the private sector that were under South Korea's Network Act and the Korea Communications Commission, that was essentially thought to be too narrow to provide meaningful benefits to EU-Korean trade. The PIPC was made the central administrative agency with independent authority over all situations of processing personal information. The PIPC also has the power to investigate violations and enforce fines and sanctions. The second is to deal with anonymised data under the PIPA, rather than in separate guidelines with no clear legal status, and the third to introduce a data portability right, which has eventually been added into the PIPA. The South Korean Government are in the process of gradually operationalising and extending their application to most of this.

**Baroness Anelay of St Johns:** You have given a flavour there of some of the differences that will arise in negotiations by each country with the

EU. In thinking of the result of all that, what is your assessment of some good practices that have come out of that which the UK should take account of and, perhaps, think about when we continue to make sure that we have data equivalency with the EU?

***Josh Lee Kok Thong:*** With respect, I suggest that the best practices that the UK may wish to consider from the experiences of Japan and South Korea concerns less the "what" and more the "how". The UK already has the UK version of the GDPR, which means that, even starting from a first-principles basis, the UK is already much more aligned with the data protection regime of the EU compared with many other jurisdictions globally. Also, the UK is in a different position from the situation with Japan and South Korea, when they were negotiating the adequacy arrangements. The UK already has an adequacy arrangement, whereas Japan and South Korea had to start from scratch.

None the less, the Japanese and South Korean experiences suggest that there may be some aspects that jurisdictions can have in mind when negotiating cross-border data arrangements with any Government. We say that factually and objectively and with utmost respect to all parties. First, what is clear from the experience is that the Governments of both jurisdictions would have had in place a long-term plan to negotiate with the EU to obtain adequacy, which their Governments then continued to track and follow over the years.

Secondly, this was backed by political will to see the plan through. It took the need to introduce repeated legislative amendments, and there was government restructuring—for example, in the case of Japan, where enforcement powers were centralised under the PPC, and in the case of South Korea, where the PIPC was brought under the umbrella of the Prime Minister's office—as well as moves that could potentially have been unpopular with civil society, the business community and society at large. For example, Japan had to remove the small business exemption and South Korea harmonised the data protection regimes for online and offline businesses.

Thirdly, there is wisdom in the approach of having a coherent, unified and sensible trade and data protection regulatory approach, such that international trade law and data protection law can be reconciled. That can be seen in the case of the EU-Japan adequacy decision whereby both jurisdictions could reap the benefits of both the adequacy regime and the economic partnership agreement that was announced a year before the adequacy decision was announced. To this end, I would venture to quote Professor Paul Schwartz from Berkeley Law in his observation that: "In general, the disjunction between trade law and data privacy law rests on a lack of coordination between institutions that negotiate trade and those that negotiate data privacy". I hope that that answers your question, Baroness.

**Baroness Nicholson of Winterbourne:** Thank you very much, Mr Josh, for elaborating so clearly the distinct difference between data protection

in the European Union member states and in the UK and Japan. I think that I am probably correct in saying that we started with data protection in 1948 with the rights to privacy for the family, and you did not really begin until about 1988, when you brought something forward from the scientific committee of your parliament on protection of scientific data. This gives rise to your twin-track process. Do you think that there will be a harmonisation of that process? In fact, that rather fits your thinking. I wonder whether you are going to continue in the way that it is without having the overwhelming data protection, which I think is amazingly ineffective nowadays, which the western European Union and UK follow, and to a certain extent the USA.

***Josh Lee Kok Thong:*** I understand that you are asking about the Japanese situation, whereby you have a track for data that originates from Japan as well as data that originates from the EU. Based on what we understand of the circumstances, our understanding is that it is likely that that situation will continue for the foreseeable future. This goes down to the cultural, legal and historical context. We see are seeing two very different regimes, in the EU and Japan, coming together, and this is not something that we can change overnight or with the blink of an eye. To answer your question, I think that the situation will continue, although it remains to be seen what happens over repeated instances of the adequacy review that goes on between the EU and Japan.

Q77 **Baroness Lawlor:** In 2011, a number of countries developed the cross-border privacy system—CBPR. As far as I understand, nine economies now belong to it, including the US and Canada. In your view, what are the advantages of it? I gather that it is a certification system that companies join voluntarily—so that sees to the commercial side. What are the advantages of it, as you see, from the US point of view? What can the UK learn from it and how does it differ from the EU system?

***Professor Peter Swire:*** The Cross-Border Privacy Rules started as an Asian effort. Currently there is discussion about raising the standards of data protection under the rules. Unless that happens, it will be hard for the CBPR really to affect the rest of the world, because the current standards are pretty old and nondescript.

The UK has a chance to be a bridge between different parts of the world. There is a puzzle for privacy that we have not discussed yet today: there are standards at the EU and UK level and then the OECD for government access has a series of standards. Then there are another 50 countries after that—what are they going to do? What is Malaysia going to do?

Then there are the authoritarian countries at the far end, where we do not have trust. There has been almost no global progress on what I call the next 50, but it might be the next 100 or whatever, countries. They have been left out of the international discussions, so some kind of multilateral way to move forward for those many countries seems to me an essential part of how a global system would operate. The CBPR is a way in which that can happen more than would happen under an EU adequacy approach. I see it as a process towards possibly expanding the

scope of countries that can have close enough harmonisation that they can work together.

**Baroness Lawlor:** Splendid. And the US?

***Professor Peter Swire:*** I think the European Union has seen the US as trying to have CBPR as a counterweight to GDPR. If that was the US strategy, it has not worked. GDPR has won. Many countries have more or less copied GDPR. That said, we are going to have to move to a next generation of all these other countries having some way to trade with each other. Lots of trade is not going through the EU. If Malaysia trades with the Philippines, India or Africa, none of that is EU-based. CBPR has the opportunity to become a collection of countries that might find ways to raise standards to develop confidence free-flowing with trust. That is the vision that the US would see for it now.

**Baroness Lawlor:** And you would see the UK as a potential leader in that?

***Professor Peter Swire:*** The UK has historical ties to many of the countries I have just named, and knowledge of and business relations with them, and all those things.

***Josh Lee Kok Thong:*** I want to mention for context that just last week, I represented the Future of Privacy Forum at the global CBPR forum workshop in Tokyo. Today I find myself in Seoul, South Korea. It is very interesting that over the course of two weeks I have been in both jurisdictions that we are discussing today.

A point I want to raise from my observations from the global CBPR workshop in Tokyo is that there were two words that kept being shared: "network effects". Network effects refer to the phenomenon where the more people or parties you have on board a particular network, the value of that network grows exponentially. That network effect summarises the promise, idea and policy of the CBPR system. The real test of that comes down to the implementation.

That segues into my next point, where I agree wholeheartedly with Professor Swire. The UK can potentially position itself as a leader in the conversation on cross-border data transfers globally and internationally, given its specific position. I will provide a bit more detail right now.

I want to highlight that prior to the enactment of the GDPR, there was an effort by the Article 29 working party of the data protection authorities in the EU and the APEC electronic commerce steering group data privacy sub-group. The effort was to cross-map the compliance and certification requirements of the EU's system of binding corporate rules—BCR—and the then APEC CBPR system. I note as well that the APEC CBPR system and global CBPR are substantially the same, for the purposes of our discussion today. We also understand that the UK was leading efforts of the Article 29 working party at the time.

This suggests to me that the UK is in a highly unique position as a jurisdiction; first, with a data protection regime that is significantly similar to the EU GDPR. Secondly, it has an adequacy decision with the EU. Thirdly, it has experience negotiating EU BCRs and the CBPR system. Fourthly, it is an associate member of the global CBPR system at present. This means that the UK is one of a kind in the world, if I may say so, to potentially take a significant leading role in exploring the interoperability between the CBPR system as well as the GDPR regime.

**Baroness Lawlor:** What are the implications for our relationship with the EU's GDPR of the UK joining the CBPR?

***Josh Lee Kok Thong:*** I can take a first stab at that question. I think that this is a stab in the dark. It is hard to say for sure what the implications will be because we are also having to think about what the EU will think about in its considerations, should the UK go for a full membership status under the CBPR system. I think there is also potential for the UK, as I mentioned, to play a leadership role in trying to negotiate and navigate the intersection between the two systems. I make that quick point and wonder whether Professor Swire has anything to jump in on.

***Professor Peter Swire:*** In this case, Josh was at the conference last week in Tokyo and I certainly was not. I really rely on what he said.

Q78 **Lord Jay of Ewelme:** You have already said or implied a certain amount about the EU's approach to adequacy, but I wondered whether you could say a little bit about your overall assessment of the EU approach to adequacy, and whether you think it is a sustainable model in the long term. A little more broadly, could you very briefly say something about your perspectives on a more effective and efficient global system? I know that Professor Swire has already said something about that, but that will be very helpful.

***Professor Peter Swire:*** I did say different points, perhaps.

**Lord Jay of Ewelme:** Let us go to you first, Professor Swire.

***Professor Peter Swire:*** The EU system is asking a great question about whether the US or the UK meet the strict legal standards. I do not know how people in the EU think that there can be trade with China, India or many other countries that do not have anything like the limits on surveillance that the UK and the US have. When it comes to government access, I simply do not understand how lawyers sign the ability to send personal data from Europe to China. Germany and China recently signed an agreement on autos to share all sorts of data together. I am baffled. As a law professor, I cannot understand that.

There is a different issue about adequacy that we have not mentioned. Other countries and jurisdictions also have adequacy. Everyone is tempted to have adequacy because if you are going to protect your own people, you want to protect them when their data goes elsewhere and

only to protected places. But we cannot have 200 countries of the world doing assessments of 200 countries without thousands and thousands of adequacy decisions. It just does not scale. Over time, there will be enormous hope that we can find international ways to do things. The biggest concrete achievement on that at the OECD has been the trusted government access principles, which the UK and US were very involved in. The EU and member states were very much in the room for that. Those give a path to having—at least for rule-of-law democracies—a way to do these things, but I do not know how Europe thinks that it is going to do business with China going forward.

***Josh Lee Kok Thong:*** To go back to the earlier question regarding the impact of the UK joining the global CBPR as a full member and its impact on the adequacy efforts, I regret that I need a little bit more and would draw a line across the entire point. Participating in the CBPR system will not necessarily preclude a jurisdiction from obtaining an EU adequacy decision on maintaining its adequacy status. Real-life examples in APEC are Japan and South Korea, which both have an EU adequacy decision and currently participate in both the APEC as well as the global CBPR systems. Both jurisdictions have fully implemented the CBPR system. They have appointed accountability agents and they have both issued CBPR certifications for businesses.

None the less, to ensure that there is no negative impact on the UK's adequacy status, the UK should consider providing both legal and political assurances that participation in a global CBPR system would not lower the level of the data protection in the UK below GDPR standards, especially when it comes to issues such as onward data transfers of EU-originating data. To this end, it is a truism, but regular dialogue and review of the arrangement and co-operation with the EU would be essential to addressing any concerns.

Let me just reiterate the FPF's overall position. Our position is that we take a balanced and broad-tent approach to all cross-border data transfer mechanisms. We see that it is important for all these systems to interoperate with each other in a way that enhances cross-border data transfers while respecting the legitimate policy considerations of Governments. This is essential.

That helps me turn to the final question that was asked. The EU's approach to data adequacy is not solely the EU's approach any longer as this type of requirement has proliferated to various extents globally through enacted laws. At least 85 jurisdictions around the world empower a regulator or government agency to designate other jurisdictions as having an adequate level of protection.

At the same time, it should be noted that adequacy is merely one tool in the toolbox of data protection regulators and regimes that allow cross-border data transfers of personal data, alongside and in parallel to adequacy: the standard contractual clauses, certification mechanisms, BCRs and even content. These are all possible avenues that allow for

cross-border data transfers, both in the GDPR and in most jurisdictions that provide for rules on international data transfers.

The biggest advantage of a jurisdiction having been adequate is that all transfers of personal data can flow unrestricted without any other formalities, as I mentioned earlier. So there are advantages to this particular tool. Conversely, entering model contractual clauses or going down the certification route could be the preferred solution for some organisations in particular contexts for transfer.

I reiterate my earlier point: the UK is in a unique position vis-à-vis the adequacy system under the GDPR as well as the CBPR system. This ability to display legal as well as political nous in this context could extend the UK's leadership and thought leadership, especially with regard to cross-border data transfers globally.

**The Chair:** We have just gone over the hour but I believe that Professor Swire can stay until half-past; we promise to release you then, Professor. Lord Hannay, who is visiting from the International Agreements Committee—it is also launching an inquiry into trade and digital—will ask the last question.

Q79 **Lord Hannay of Chiswick:** I thank the whole committee for allowing me to come along on this occasion—back to my old haunts.

First, I will say a word about the International Agreements Committee, which is conducting a short inquiry into the digital trade element of the free trade agreements that the UK either has negotiated—with Japan, New Zealand and Australia—or wishes to negotiate; for example, with India and Turkey. Subject to the former chair of the International Agreements Committee, who is sitting three to my left, one question that it occurs to us to ask you is: do you think there are any tensions between the UK actively pursuing a digital trade chapter dimension in its free trade area agreements and its ability to retain the EU adequacy ruling when it comes up for review? Obviously, that is extremely important to the UK. I am not suggesting that we have come to a view that there are such tensions, but I noticed that Professor Swire said that, if you have an increasing number of spaghetti-like bilateral deals, it becomes a bit self-defeating at a certain point—that may be part of the answer to my question.

Secondly, both of you spoke about wider multilateral or plurilateral agreements, as you could call them. Last week, in the evidence that we took in the International Agreements Committee, we were told that there is some prospect—no more than that—of the World Trade Organization being able to agree some basic rules. These would not be as sophisticated as some of the bilateral ones we are talking about but would nevertheless meet the need, which both of you have suggested exists, to bring more countries into the game.

Can you comment on those two things: the possibility of tensions between the UK's bilateral deals and its data adequacy ruling by the EU; and the prospects for and desirability of some wider arrangement,

perhaps through the World Trade Organization?

**The Chair:** All that in 10 minutes between you.

***Professor Peter Swire:*** On the first point, there is a tension. Each country is sovereign and understandably wants both to have rules that apply to its own people and to decide how to do that. The UK has made the decision not to be part of the European Union, and wants freedom to do the various things that it thinks are the best things to do, but, as there is deviation from the GDPR—and from the charter, if that happens—there is an increased risk that the Commission might be upset and, even more so, that the Court of Justice might find the deviation too large. This would, in essence, make Britain no longer equivalent.

The discussions here are not just among diplomats, economic and business experts and privacy experts and not just about what the best regime is. It is about what will survive fundamental rights scrutiny by the court, which has been very strict so far. For instance, if the bilateral agreements led to onward transfers without appropriate protections, the court might find that the rights of Europeans are not being respected when the data gets to the UK. That would be a concern, right, because EU data comes to the UK and now it goes out the door to who knows where. Those bilateral agreements could involve a lot of EU citizen data. That is a concern. The risk is that the court would think that the protections are not good enough.

I have a couple of observations on the WTO point. One is that, in previous negotiations—on services, for instance—the EU consistently insisted on quite a large exception to give nation states the ability to write privacy laws. So there is quite a lot of room for the EU to do what it wants to do on GDPR, consistent with current WTO standards.

The limit on that is if there is discrimination. For instance, if it were to say no to a country with good standards and yes to a country with bad standards—say, the US and China, when it comes to government access—it could lead to a discriminatory application claim, which is where the WTO system might find a violation.

The second point on the WTO is that there was a mysterious shift in US policy in the last year or so about trying to have a free flow of data in the WTO instruments and other plurilateral instruments. There are mixed views within the US Government right now, but at least some in the Government, including the trade representative, have said that the US needs more room to write its own national rules about data flows and that the US Government are no longer as much of a supporter of the free flow of data as they were for the last forever years.

I do not know how far and long that change in US policy towards the WTO will continue, but the US, even with its China trade issues, is cutting off data flows for the first time, in a way that we have not seen before. The WTO may be a difficult place, because even apparent allies might not be fully aligned on what to do with it right now.

***Josh Lee Kok Thong:*** I shall answer these questions quickly. I am not an international trade law specialist, by any stretch of the imagination. On the second question, I probably defer to what Professor Swire just said. But in response to the first question, I will add to what Professor Swire said as, yes, there is a tension but it is not unnavigable. It can be navigated.

I point back to the instance of the EU-Japan data adequacy arrangement, which was a reconciliation of the international trade dimension, as well as the data protection and data transfers dimensions.

Another example is the digital economy agreement that was agreed between the UK and Singapore, as well as the digital trade principles between the EU and Singapore. In the UK-Singapore digital economy agreement, Article 8.61-G recognises that each party may have its own regulatory requirements concerning the transfer of information and that "Nothing in this Article shall prevent a Party from adopting or maintaining a measure inconsistent with" the paragraph above "to achieve a legitimate public policy objective". The agreement basically says that it wants "to encourage the development and adoption of mechanisms to promote compatibility and interoperability between" different data protection regimes. This could include "mutual arrangements … or broader international frameworks".

I basically want to say that it is possible to balance such provisions in international agreements to encourage data flows, while respecting legitimate policy imperatives to maintain protections over personal data. Legal standards and safeguards can be put in place, such as arbitrariness or unjustifiable discrimination, or elements such as necessity. You can see some of this wording in the EU-Singapore digital trade principles and the UK-Singapore digital economy agreement.

**Lord Hannay of Chiswick:** Do the provisions in the EU-Japan and UK-Japan agreements meet that kind of gold standard?

***Josh Lee Kok Thong:*** I am not privy to the trade agreements between the EU and Japan but would be happy to get back to you in writing on that point.

**The Chair:** Thank you both very much. We have made the 5.30 pm deadline. Josh, I have no idea what time of night it is in Seoul, but it is very late, so thank you very much for staying up so late and giving us a very rich and useful evidence session. It certainly helps our inquiry, so we have greatly appreciated it. If either of you thinks of something you want to supplement to it, by writing a further note, we would be happy to have it. For now, I end this public evidence session with warm thanks from the committee.