HOUSE OF COMMONS

International Trade Committee

Oral evidence: Digital trade and data, HC 1096

Wednesday 10 March 2021

Ordered by the House of Commons to be published on 10 March 2021.

Watch the meeting

Members present: Angus Brendan MacNeil (Chair); Mark Garnier; Sir Mark Hendrick; Anthony Mangnall; Mark Menzies; Lloyd Russell-Moyle; Martin Vickers; Mick Whitley.

Questions 53 - 80

Witnesses

I: Professor Christopher Kuner, Professor of Law, Vrije Universiteit Brussel (VUB) and Co-Director, Brussels Privacy Hub; Professor David Collins, Professor of International Economic Law at City, University of London; and Dr Kristina Irion, Assistant Professor, Institute for Information Law (IViR), University of Amsterdam.

Examination of Witnesses

Witnesses: Professor Christopher Kuner, Professor David Collins and Dr Kristina Irion.

Q53 **Chair:** Welcome to the International Trade Committee's second hearing on digital trade and data. We have two panels today, a panel of three and a second panel of three. In the first panel we have Professor David Collins, Professor Christopher Kuner and Dr Kristina Irion. I would like each of you, starting with Professor David Collins, to introduce yourselves—name, rank and serial number—in your own terms.

Professor Collins: My name is David Collins. I am professor of international economic law at City, University of London. I specialise in all of the World Trade Organisation and international investment law.

Professor Kuner: My name is Christopher Kuner. I am a law professor at the VUB, which is a Flemish university in Brussels. I am also a visiting professor at Maastricht University. I specialise in EU data protection and privacy law, and also global data protection privacy law and internet regulation.

Dr Irion: Greetings from Amsterdam. I am Kristina Irion. I am assistant professor at the Institute for Information Law at the University of Amsterdam. I specialise in global data flows and the governance of transnational technologies. I am glad to be here.

Q54 **Chair:** Thank you very much for joining us from Amsterdam. I am in the Hebrides, and I hope the weather in Amsterdam is a little better than we have here in the west of Scotland at the moment.

I will kick us off with a brief question before I move on to colleagues. First to Professor Kuner, what is meant by "data privacy" and how is it relevant to digital trade?

Professor Kuner: First of all, let me thank you very much for inviting me. The issues to be discussed here, of course, are highly complex and we have little time. I will thus be very brief in trying to be succinct in my remarks, even at the risk of missing some nuances, which I will most likely do. I should also add that I am a lawyer and law professor, so my answers are based on my evaluation of the relevant legal issues. I will stay clear of any political issues and leave that to all you MPs.

Yes, a very good question, a difficult question to answer briefly, but let me try. First of all, as to what is data privacy, there are different conceptions of this term in different legal systems. Even the terminology differs between regions. In the EU we have the term "data protection", which is also the term used in the UK. In the US they refer to "privacy", but I think for the purposes of this testimony, we can regard these terms as synonymous. Broadly speaking, data privacy can be understood as embodying three main concepts: first, that individuals have rights in data that can be used to identify them; secondly, that there must be a legal

framework in place to provide—I would call them—rules of the road for data processing; thirdly, that there must be remedies that an individual can exercise if a party, whether in the public sector or the private sector, violates these rules. The reason that we provide legal protection for data privacy is that processing of data that identifies you may have serious implications for individuals, for their dignity as a person and it can also lead to all sorts of harms, including misuse of data in ways that violate your expectations, discrimination and even serious human rights violations.

On the second part of the question, data privacy is very relevant to digital trade, again for three main reasons. First, digital trade seeks to promote commerce and the international exchange of data, while data privacy restricts the processing of personal data to protect individuals. Therefore the two sometimes stand in tension with each other. Secondly, I think most trade today is unthinkable without also involving the processing and transfer of data in some form. Finally, data privacy can facilitate digital trade by increasing the confidence of individuals and enterprises in the cross-border digital exchange of data. I don't think we should think of it as just trying to hamper trade. Thus, I think that data privacy and digital trade are inextricably intertwined.

Q55 **Mark Menzies:** Christopher, back to you for my first question. What are the main differences between the EU and the United States in their approaches to regulating digital trade and data privacy?

Professor Kuner: Again, a difficult question but a very good one. I should also say that data privacy is a global concept now and many countries—probably the majority of countries—around the world have laws protecting it. Let me try to give a brief response. I would not want to give the impression that there are only differences between the EU and US approaches. Of course, these are two of the main approaches around the world. In fact, I would say they have been gradually growing closer together over the last few years and have even influenced each other, but still there are fundamental differences in these two approaches.

Again, this could be the subject of weeks of testimony, but let me just highlight maybe three main differences. First, the EU approach to data privacy is based on recognition of it as a fundamental right at the constitutional level, so at the highest legal level with regard to violations in both the public and private sectors. In the EU, data protection receives constitutional protection and also in the private sector. In the US, however, privacy is also considered a human right but it is protected at the constitutional level only with regard to action by the state, action by the Government, and not by the private sector.

Secondly, these differences at the constitutional level mean that, in the EU, violation of data protection is seen as a human rights violation. Its protection is largely assigned to special independent public authorities, known as data protection authorities, and of course in the UK you have

one of the best data protection authorities, the Information Commissioner.

In the US, by contrast, data protection in the private sector is governed not by constitutional law but is seen largely more as a transactional matter and is based much more on mechanisms agreed between private parties, such as contractual agreements and compliance with online privacy policies. Thus, while enforcement of data privacy by consumer protection authorities certainly exists in the US, it tends to be based much more on violation of contractual commitments rather than on human rights law, at least with regard to the private sector. This is a different matter with regard to the public sector there.

Thirdly, the EU has a legislative framework for data protection that applies horizontally across both the public and private sectors. The US has a lot of legislation on data privacy, but it tends to apply more sector-by-sector, so covering, for example, health data and is thus more fragmented than in the EU. There is, however, very lively discussion going on in the US about the potential need to enact some horizontal legislation covering data privacy at the federal level.

Q56 **Mark Menzies:** Thank you, Christopher. David Collins, how do these approaches compare to the approach taken by China?

Professor Collins: China started to develop its data privacy framework much later than the EU and US. You can see this in its internal policy and through its trade agreements covering digital trade, where free flow of data really only began to appear in the last five years or so. I think China started to look at this more seriously because of the emergence of cloud computing and big data, and so on. Unlike in the EU, data privacy rights in China focus solely on consumers. Citizens don't enjoy the same level of protection as part of their civil liberties. Like the US, China scatters data protection across various laws. More recently it has widened the scope of its rules and is now potentially on the verge of adopting a comprehensive law on data privacy like that of the EU.

Generally, the central features of China's model for data privacy are national cybersecurity and an emphasis on the separation between privacy from private actors, which is more protected, and privacy from the state, which is poorly protected. This obviously clashes with the EU's view of privacy as a fundamental right. China is getting closer to the EU on privacy. We are seeing various safeguards for sensitive data, such as requirements that the processing of personal information is only for the purpose initially specified to the individual.

Interestingly, some of the progress that China has made is through non-binding texts and guidelines, and that is in keeping with the Chinese legal tradition, which is also quite vague and prone to generality. We have privacy rules basically being part of a complex framework across various laws and regulations in various sectors, and so on. I will not mention some of the specific ones, but I want to mention that many of the

guidelines are technical in nature and cover issues like data transfers, sensitive personal information and data subject rights. Again, they are not legally binding, but in the Chinese legal system they can be highly persuasive and the protections will depend on the type of industry, the type of information involved, whether it is personal information obtained by financial institutions, personal information collected by telecoms or internet service providers, and so on.

I mentioned that China appears to be moving toward comprehensive privacy law like the EU's GDPR. In October of last year, a draft personal information protection law was published for consultation. That would be the first of its kind in China and would create binding compliance obligations, which would be interesting.

Finally, to get a sense of where China is at with privacy rights in its trade agreements, the interesting thing with China is that it has not made as deep commitments to the free flow of data as many other countries have done in their free trade agreements. For example, in the RCEP, the Regional Comprehensive Economic Partnership agreement that came out late last year, the electronic commerce chapter has massive gaps in it, which allow the Government to enact all kinds of policy measures for national security or whatever reason. I think in that sense there is quite wide latitude to potentially fit privacy objections in there.

Q57 **Mark Menzies:** Kristina, to what extent is there still a clear distinction between these different approaches?

Dr Irion: Christopher Kuner was correct to highlight that the constitutional and fundamental rights approach that is leading in the EU is a clear difference to how it is done in the US and also in China. But adding to that, one important difference is that there is a clear public-private divide in the US legislative framework, that is to say that there is a specific governance mechanism to protect US citizens against US Administration infringements into their privacy. That is the fourth amendment protection. Consumer privacy or the private sector relationships between citizens and businesses operate under a totally different framework and different rules, which are patchy, as Professor Kuner said.

In the EU it is more like a comprehensive and horizontal approach, so the same rules apply to the private sector and public sector, which pulls it all up to the level of protection envisioned by the charter.

There is one other very important distinction between the US and Europe, for example, and that is how they approach cross-border transfers of personal data. In its GDPR, the EU has rules to regulate the transfer of personal data to third countries, quite specifically so. These safeguards are in place to avoid the circumvention of the protection afforded to personal data in the EU once it has been transferred to a third country. This is different in the US, where cross-border transfer of personal data is currently unregulated. However, here we are also seeing some

developments, especially since the US is no longer the only power in online commerce and online digital services. There is now currently a stronger understanding of personal data of US persons becoming a potential national security issue for the US, not vis-à-vis the EU, more vis-à-vis China, for example.

Mark Menzies: Thank you, everyone.

Q58 **Mark Garnier:** Kristina, I will continue with you. You made reference to GDPR. What I am particularly interested in is how the EU and the UK seek to protect data privacy in the context of digital trade using GDPR. How successful do you think they are in doing so?

Dr Irion: I speak as a lawyer. The GDPR takes a formulistic approach—I borrow this phrase from Professor Kuner—to regulating cross-border transfers of personal data. It has a menu of alternative options to transfer personal data. The best-case scenario for the UK is an adequacy decision, because with an adequacy decision a third country is kind of assimilated into the internal digital market of the EU and can freely receive personal data from the EU without any further safeguards.

That can only be granted if the level of protection of the third country is essentially equivalent to the level of protection afforded in the EU. That involves quite intricate testing of many factors of the legislative and legal systems of the third country. However, it does not need to be one-to-one identical. Essentially, equivalent means that the main tenets of EU data protection law that Christopher Kuner rightly described, with individual rights, with independent oversight and so on, are reproduced in the legal framework of the third country.

Where there is no adequacy decision, there are still a number of alternative safeguards to transfer personal data. This is mostly grounded in contract law. For example, organisations can receive personal data from the EU or from the UK at the moment when they conclude a contract, a so-called standard contract on data protection, where they agree to protect the data after it is received, according to similar provisions that we would find in the GDPR currently. This would then be embedded in a contractual relationship between the exporter of data and the receiver.

Finally, there are some derogations from these rules. In individual circumstances it will be possible to transfer data, for example, based on the consent of the individual concerned, but this is only used when all other mechanisms don't function. On the relevance in practice, you know that there are not so many adequacy decisions at the moment. These are long procedures that lead to an adequacy decision, which can take several years. We have currently, if I am not mistaken, 16 adequacy decisions. A number of them are small islands in not very relevant territories, but of course the adequacy decision with Japan is the latest, bigger, new one under the GDPR framework.

This is the highest level of recognition that can be achieved under the GDPR, and we exchange personal data with many countries outside of the adequacy framework using the contractual safeguards. This works fine. However, there is criticism that countries are not receiving the same even-handed treatment.

Q59 **Mark Garnier:** Can I be clear on the difference between adequacy and equivalence? As I understand it, the first stage is that the third country has equivalent objectives in its regime as GDPR, if not identical, but what would happen if that country subsequently changed its data privacy rules and, therefore, fell out of the equivalence regime?

Dr Irion: I think they are almost used synonymously. Adequacy is the name of the decision, but to be eligible for an adequacy finding, the third country has to be found to have an essentially equivalent level of protection to what the GDPR provides. The words are kind of synonymously used, but to have an equivalent level of protection, it does not need to be a word-for-word reproduction of the EU legislative framework. There is some variance possible. It is about the main tenets of the protective framework, which need to be found in the third country as well.

Q60 **Mark Garnier:** Going back to my question, if that country, having done a trade deal, subsequently changes its rules, what happens? Do you fall back on contract law as a way of doing trade?

Dr Irion: There are several steps involved. If a third country enters into, let's say, inconsistent commitments, on the one hand with an adequacy framework that has a higher standard, and maybe on the other hand a trade deal that has a different standard, often lower, for cross-border transfers of personal data, this country is in a situation of inconsistency. The adequacy framework would need to be reassessed. If this new trade agreement threatens the essential equivalence finding, this could affect the adequacy framework.

On the other hand, in international trade law there are also enforcement mechanisms. A country that is trying to do both at the same time, without carefully calibrating that they fit together, could also find itself in a trade law dispute with yet another third country that is saying, "Yes, but your adequacy framework is treating me on less favourable terms and I would like to receive your personal data without this high level of data protection attached."

Q61 **Mark Garnier:** David or Christopher, do you have anything to add to that? In particular, do you think the EU and the UK are successful in protecting consumers' data?

Professor Kuner: The only thing I would add—I agree completely with what Professor Irion said—is that the essential equivalence does not have to be identical. Let's say if the UK were to change its law, having been found adequate, that doesn't mean that automatically the data flows would have to stop. It would have to explain to the EU, "We have

changed our law, but the effect is basically the same," so it does not have to remain exactly identical.

As to whether they have been successful, I think there is probably no shining example around the world of an absolutely perfect data privacy law because the field evolves quite fast, technology changes a lot, so in a way the law is always trying to catch up with the reality. But I think the EU and the UK—of course the UK legislation is now very much based on the GDPR—are regarded around the world as having two fairly high standards of protection. There is a lot more detail that one could say, but I will not go into it.

Professor Collins: My only thought is that I think Professor Irion mentioned the potential for trade disputes through most favoured nation. I am not aware of trade agreements that apply data transfer protections and privacy exemptions on a most favoured nation basis. I have not seen that in digital trade chapters. If they are there, it would depend how they are phrased. This tends to be something that is supported bilaterally, much like equivalence. I am not sure that there would be a mechanism within a trade agreement to address those kinds of concerns, but it would depend on how it was phrased. That is all I wanted to say, thank you.

Mark Garnier: Thanks very much.

Chair: Sitting here on an island of 13 kilometres by 8 kilometres to save me from the wilds of the Atlantic, Professor Irion's comment about small islands being not very relevant territories made my ears prick up somewhat, but I get the context of that. Thank you. We will go to Sir Mark Hendrick now. Sir Mark, I hope you are in a more substantial territory than I am at the moment.

Q62 **Sir Mark Hendrick:** David Collins, how does the UK-Japan agreement address data privacy issues?

Professor Collins: The UK-Japan CEPA contains, in the services e-commerce chapter, a commitment to maintaining comprehensive legal frameworks to protect personal information. That is in Article 8.80.2, if you are interested. The text of this provision is seen in a lot of these treaties. It says, paraphrasing, that the parties recognise the economic and social benefits of protecting personal information. Then it goes on to say that each party shall adopt or maintain a legal framework that provides for the protection of personal information.

It adds to that through a footnote, which says that a party can comply with that obligation to provide a framework to protect privacy through personal data protection laws like the GDPR, sector-specific laws covering privacy like the US, or even laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy, which Australia does to a degree. That is the main provision, but again all that talks about is just establishing a framework. It does not create rights or create a facility through which individuals could potentially exercise how their

privacy rights are safeguarded. These provisions are enforceable through the state-to-state disputes settlement chapter of the agreement.

From there, we see the general exception provision, which allows for the restriction of data flows for the protection of privacy and that is modelled on the WTO GATS agreement. I think we may be talking about that later. Data privacy is also contemplated by Article 8.84 on cross-border transfer of information and Article 8.85 on the location of computing facilities. These provisions are basically framed in the same language. It starts by saying the parties cannot restrict electronic transfer or they cannot require local computing facilities.

However, "Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 1 to achieve a legitimate public policy objective", which presumably could cover privacy. Then we have familiar language that says that it must not be applied in a manner that would be arbitrary or unjustified. That is again back to the GATS language. Those provisions relate to business activities. It is about consumer protection. Again, they are enforceable through CEPA's state-to-state arbitration mechanism.

Interestingly, just as a final point, the data localisation prohibition and the data transfer provisions don't apply to Government procurement or Government-controlled information, or they are not sweeping anyway.

Q63 **Sir Mark Hendrick:** As I understand it, the EU has a different arrangement with Japan. When Liz Truss appeared before this Committee, she was keen to highlight this particular aspect of the agreement. How does our position with this agreement differ from the EU's, and is it a better agreement for that reason?

Professor Collins: That is a difficult one for me to answer. I think I will pass this over to one of my other panellists, but what I can say is that the e-commerce chapter in the EU-Japan agreement does not cover as many types of technology as you see in the UK-Japan agreement. The UK one goes a bit further in the types of transactions that it covers, but I will leave it to one of my colleagues to comment on the EU-Japan relationship.

Professor Kuner: I think Kristina is the real expert here. I will let her go.

Dr Irion: In the EU-Japan agreement at this moment there is a so-called rendezvous clause, which means that there is no provision on the cross-border transfer of data. The reason is that after so much political discussion in the various EU institutions, the Parliament, the Commission and so on, there has been a compromise found that the transfer of personal data should be handled using the GDPR mechanisms instead of using trade law.

To not confuse and conflict these two different legislations or different ways of governing cross-border transfers of personal data, the EU has resolved that it does not need that in the trade agreement with Japan. The day that the trade agreement was signed was also the day that Japan granted the EU an adequacy decision and the EU, on the other hand, granted Japan an adequacy decision. It shows that the EU is trying to keep personal data outside of its trade agreements. However, there is now a different language in the EU-UK Trade and Co-operation Agreement.

When I look at what the UK and Japan have negotiated in their agreement, you have basically agreed to a trade law commitment to the free movement of personal data between the UK and Japan. You have introduced an exception to this commitment, and this exception reads "necessary to achieve a…public policy objective". One of these public policy objectives can be privacy.

Q64 **Sir Mark Hendrick:** Are you saying that the arrangement that we have with Japan is more relaxed, whereas the Europeans think GDPR is the answer to all these problems and it should be done through what they regard as a gold standard GDPR rather than a trade agreement?

Dr Irion: Yes, that is right. It is more relaxed, simply because trade law follows slightly different rules and has the possibility to give preference to a trade objective, as compared to the GDPR, which is geared to what is a fundamental rights objective.

Q65 **Sir Mark Hendrick:** That might be good for trade, but is it good for personal private data? Is that the question?

Dr Irion: Reconciling both requires that data privacy is ingrained inside the data flow. It is always easier to agree to a free data flow commitment and leave the protection to the other party where it arrives. With Japan, this may be all right because Japan has a pretty strong data protection framework and it is, for example, recognised as essentially equivalent by the EU. The risks are, in that sense, probably much more hedged, yet it comes with the onward flow of data that the risks can become more tangible. Data originating in the UK that is transferred to Japan using a mechanism—for example, your trade agreement—could, once it is in Japan, travel onwards, because Japan has made many different agreements that commit to a free data flow.

Sir Mark Hendrick: It could go anywhere, even though the Japanese have treated it quite well. All right, thank you.

Chair: Moving now to the Liverpool area with Mick Whitley.

Q66 **Mick Whitley:** Good afternoon to all the witnesses. My initial question is for Kristina. The UK-Japan agreement allows for limits to data flows where such limits are necessary to achieve a public policy objective. Could you explain what is meant by this exception?

Dr Irion: This is very important because it describes the extent to which a country can exercise its regulatory autonomy, although it has committed in trade law to certain rules. The general exceptions are exactly the space that is given to a country's regulatory autonomy or sovereignty, if you want. It does not come unlimited, but it is subject to certain trade-conforming conditions. What we find now in the UK-Japan CEPA is a formula, a language, that we know from all other trade agreements that goes back to WTO law. It is an accepted formula in trade law.

It introduces a certain legal test or, let's say, a threshold that a domestic regulatory measure, such as in the field of data privacy, has to meet to be justified in trade law. A country that introduces data protection law that would contradict, in one way or another, the cross-border data flow commitment it has entered into has to justify its data protection law. The threshold is necessary to achieve a public policy objective, and "necessary to achieve a policy objective" is regularly interpreted by trade law bodies that it should have a connection between the objectives and the means of these domestic policies, so this is straightforward.

There must be a logical link between the two, but "necessary" also means that there should not be other, less trade-restrictive alternatives to achieve the same policy objective. Since such a discussion would take place in the trade law forum, it invites alternative ideas on how exactly to regulate the cross-border transfer of personal data. As we know, there are several competing approaches to the regulation of cross-border transfers of personal data out there at the moment. There is nothing like an internationally accepted standard of how to do that, and there is a very high approach of the EU and the GDPR, which is also currently in the UK, that means there are adequacy instruments and special safeguards when personal data is transferred to a country.

There are other, much less trade-restrictive approaches in, for example, the Asian cross-border privacy transfer rules. Also here, basically, it is much less cumbersome and you could argue that justifying GDPR-style cross-border transfer rules would be hard using the necessity test. There is a residual legal risk that GDPR-style legislation cannot meet the justification of the general exceptions, and that would mean that such a measure would, in the end, contradict a trade law commitment.

Japan is quite interesting in that sense, because Japan has joined every possible international agreement and method to export and receive personal data. It uses trade law, it uses the Asian cross-border data transfer rules and it is using adequacy instruments with the EU, so it is basically a member of every club out there. It is difficult to imagine how this can be reconciled internally in how they all work together. In that sense, what Japan is doing is not very consistent and it will show at some point.

Mick Whitley: Thank you. David or Christopher, would you like to

contribute to that?

Professor Collins: Yes, there are a few comments I would like to make. I am not sure if I am going to be asked about this later. I want to add that the necessity test for general exceptions in services comes out of the GATS agreement, as Professor Irion alluded to. The general exceptions in WTO law have always been a very high standard to satisfy. There have been about 40 cases, and I do not think any was ever successful. There has been one case brought under the services agreement, which is an analogous one in the context of what you see in the CEPA, and that was the Argentina financial services dispute. It did not concern privacy; it concerned various measures like withholding tax on transfers, and so on. It failed, as it did not satisfy the test.

Under international law, necessity is incredibly strict. It is not just that the goal relates to the means used to achieve it; it is essentially that it is the only one that could achieve it. I think in that regard it would be very difficult to get a privacy-oriented exception in there. To add to that, the mention of the WTO is not random. CEPA mentions that the dispute settlement panels should be inspired by WTO rulings. I do not think it uses the word "inspired" but it says something along those lines.

A lot of it will turn on what that dispute settlement ends up being like and how that plays out. This is the arbitration provision that governs dispute settlement for the agreement: who the arbitrators will be, the nature of the evidence that they seek, because they are empowered to seek evidence to reach their decision, whether or not there are amicus briefs from public bodies or charities that might get involved and public participation. I think a lot of it will turn on how that plays out in those tribunals.

One final point, there is so little precedent out there in the world on how dispute settlement bodies in free trade agreements operate. We have a little bit of case law with the WTO, but we do not have many under the free trade agreements. We certainly do not have any under the Japan agreement, and we do not even have any indication of what it would look like.

Q67 **Mick Whitley:** Is the exception sufficiently broad to allow the UK to maintain its current data privacy regime?

Professor Collins: The exception doesn't look like it would be sufficiently broad to do that. Let me make one final point. It is very narrow, but it is perhaps not as narrow as it could be. I say that because, if you look at the CPTPP and its prohibitions on data localisation and restrictions on transfer, there is an extra little bit there and it makes reference to the notion of there being no other way. The fact that that language is missing from the CEPA suggests that maybe there is a little more light getting in there, so there may be slightly more room than you would see under the CPTPP.

Importantly, one final point: "necessity" in the CEPA is not self-judging. It is not what the UK or Japan thinks is necessary; it is what a neutral arbitration panel thinks. Contrast that with what you see in the RCEP, where the RCEP parties get to declare what is necessary to them.

Q68 **Lloyd Russell-Moyle:** Christopher, data privacy provisions in the UK-Japan agreement state that voluntary undertakings can be taken by businesses and would be sufficient to protect data privacy, but we have received some evidence that suggests this undermines the approach that we have heard about of a rights-based approach for data privacy. Do you agree that there seems to be a conflict there?

Professor Kuner: I should begin by saying that I am not a trade law expert, as my two fellow panellists are, and I am also neither a UK lawyer nor a Japanese lawyer, so I look at this from the point of view of international law. I am aware that this issue has been raised. I have looked at the relevant provisions of the CEPA and some of the concerns that have been expressed by some groups about this provision. I think it is in a footnote to Article 8.80.

This language basically says that the obligation of each party to have in place a legal framework for data privacy could be satisfied by "laws that provide for the enforcement of voluntary undertakings by enterprises". I think, as we will see is the case with these agreements in general, that this language is open to interpretation.

I can see two possible ways of interpreting it. One is that it would be sufficient if data protection or data privacy is protected by a self-regulatory regime. This is where I think these concerns come from, and I can understand those concerns, but it seems to me that another possible interpretation might be that the Japanese administrative system relies more than our systems do in the west on co-regulation, such as trust marks and alternative complaint resolution systems. I think this gets down to what is intended here by the parties. If this is seen as a way to kind of let in self-regulation as the sole way to protect privacy, it could be seen as a threat to your system of data privacy, but I also think it could be viewed as an attempt to take the particular characteristics of the Japanese system of privacy regulation into account, which is a bit different from our system.

Supporting this view, the European Commission 2019 adequacy decision for Japan also notes or takes account of the more self-regulatory nature of the Japanese data privacy regime. If the latter is the case, I would not worry as much about it, but maybe my concern is a bit lower here because, as Kristina Irion said, we are talking Japan. Japan has been found adequate under EU standards, and the EU knew very well that Japan has this more co-regulatory system. I think this is a legitimate point to raise.

On many of these issues involving the CEPA and CPTPP, or whatever the acronym is—terrible acronym, by the way; I wish they had thought of something else—I think it would be helpful if the—

Lloyd Russell-Moyle: I believe it was the Canadians' fault, but that is another story.

Professor Kuner: Let's blame them then, I am happy to do that. I think it would be helpful if the UK and the Japanese Government provided some joint explanation of what is meant here. For example, I did not see any real explanation of this point in the explanatory memorandum to the CEPA, and this should be in there somewhere.

Q69 **Lloyd Russell-Moyle:** David or Kristina, from your perspective, are voluntary undertakings by businesses just recognising the nature of Japan's regulatory system or is it an opening of the door to a different kind of system?

Professor Collins: I will make one quick point. I think Kristina probably knows more about this than I do. I am not convinced that this is a Japanese-specific concept, because you see this language in so many of these treaties. If I am not mistaken, it is verbatim in the CPTPP and it is in the US-Japan—you have Japan again. I have seen it in other treaties, but now it just occurs to me you have Japan in the CPTPP as well. Maybe it is there at the behest of Japan, and it is all these Japanese agreements. I have definitely seen it in other agreements, so I am not convinced that it is idiosyncratic to Japan.

Q70 **Lloyd Russell-Moyle:** The difficulty is if Japan has joined every club going, you can't work out whether it is Japan's request in every club or if it is something more fundamental, but thank you, David. Kristina, do you have a perspective on this self-regulation?

Dr Irion: I think this is a reference to the APEC cross-border privacy rules, which are working on industry standards and on industry agreements mostly. In a way, what this phrase could say is, "This would be sufficient to transfer personal data if there are these self-regulatory initiatives." By acknowledging that, the adequacy mechanism is a much higher threshold. If that is sufficient, it would create a lower threshold for the transfer of personal data. It would basically give it a green light.

Q71 **Lloyd Russell-Moyle:** Could that allow Japan and companies in Japan to find a lower threshold?

Dr Irion: Trade law is addressed to states, first of all, so the thing that happens here is that, if Japan or the UK makes the cross-border transfer of personal data subject to higher rules, it could be challenged in a trade dispute, it could be challenged between the countries or even a third country could come and say, "This is not all right." What happens in the end is that the text of the agreement, which will be the main source for interpreting what every country has committed to, already suggests a lower threshold. That is these self-regulatory instruments.

Q72 **Lloyd Russell-Moyle:** Would that mean that in other trade negotiations there would be a predominance to put in that kind of weaker wording?

Dr Irion: Yes, that is a little bit how it is going. In trade law circles there is a perceived gold standard for digital trade rules. This gold standard tries to facilitate cross-border transfers of personal data with as few safeguards attached as possible, because that makes it smoother. Consider that personal data is extremely fluid, and trying to keep up personal data protection when data is transferred between countries is the hard task.

Lloyd Russell-Moyle: That sounds like it is a gold standard for trade, but the wooden spoon for data protection.

Dr Irion: Yes, and there is a gold standard for data protection. What you have is the battle in gold standards, exactly.

Lloyd Russell-Moyle: Perfect. Thank you very much.

Chair: A fascinating exchange, thank you very much. I think we are back to Mick Whitley.

Q73 **Mick Whitley:** Kristina, Japan has made commitments regarding data flows to the UK and the US. We have heard different views on whether this might allow UK citizens' data to be transferred to the US. What is your view on this?

Dr Irion: This is an important question. One way to think about it is to start looking from the interests of UK citizens. UK citizens' data could be transferred to Japan, and that is in itself fine, but once it is in Japan and has thereby left the jurisdiction of the UK, it falls under Japan's own legal framework. Japan has made commitments under different regimes, especially under trade law.

If this UK personal data is not labelled and kept separately from other personal data, it could easily be subject to onward transfer to yet another third country and from there to yet another third country. This could result in a race to the bottom, because the data would go to those jurisdictions where the least requirement is attached to how they can be used, exploited and value extracted from them. Japan is not the end of the trip for UK data.

Q74 **Chair:** Following up on that, the Brussels effect—which I think has been mentioned in the brief—is where the UK only allows its citizens' data to be transferred to other jurisdictions where it deems that other Governments provide a sufficient level of data protection. Are some citizens, under some trade agreements, getting their data more protected than other citizens? For example, are the data of the good people of Amsterdam a bit safer than those who live in—what were they called—not very relevant territories, perhaps in the Hebrides under the UK Government? Is there a difference there?

Dr Irion: With these "not relevant territories" I struggle now. I am very sorry. At the moment, it is not yet often the case that different countries' personal data are treated differently in a third country, but the EU has, for example, written inside the adequacy decision for Japan that EU data has to be stored separately from other personal data and should not be subject to onward transfer. In a way, in Japan there would be an extra labelled file for EU personal data and that would be treated somewhat differently from all other personal data that passes through and transits through Japan.

At the moment I am not aware, for example, if Japan is a massive transit country for personal data, but it would potentially develop into such a hub, given that it is a very convenient spot to bring data to and then under a different regulatory framework, such as a trade agreement, take it away again. You could imagine that it makes sense to take Japan as a new place to route data through.

Q75 **Chair:** Some jurisdictions can prevent Japan doing that by the nature of the agreement they have. Is that essentially what we are saying?

Dr Irion: That is what the EU has done with its adequacy decision. This is correct, yes.

Chair: Incidentally, I realise I have not taken any insult at all from the islands thing, given you are in the Netherlands. Although the island is small, we have at least three hills rising more than 1,000 feet above sea level, which I think is probably higher than anything in the Netherlands. Anyway, moving swiftly onwards. Martin Vickers, are there any mountains in Cleethorpes?

Martin Vickers: No. We have the Lincolnshire Wolds. Those are the nearest hills to here.

Chair: That will do us. Thank you.

Q76 **Martin Vickers:** Moving on to future trade agreements, or at least potential FTAs, would you anticipate that the provisions for digital trade that are in the UK-Japan agreement will be replicated in the UK's future agreements, particularly with reference to the US?

Professor Collins: I think the answer to that is yes, they probably will be and perhaps in their entirety, but if you are looking for a model for countries like the US and some of the other big FTAs that the UK is looking at with Australia and New Zealand and then improving the rollover Canada agreement, for example, the best place to look is what is in the CPTPP. It looks to me like that will be the blueprint for the UK's digital trade chapters going forward, which is slightly different than the UK-Japan agreement but not much. The reason I put the US into that, although the US is not a party to the CPTPP, is because it was an initial negotiator in the TPP when it was the Trans-Pacific Partnership. The US had a major role in drafting the digital trade chapter, and it is looking at what the US has done with Japan in the digital trade agreement.

Interestingly, you mentioned free trade agreements but you did not mention multilateral rules. I want to add that, as you may know, the World Trade Organisation is looking at establishing electronic commerce rules and struggling with it. I think it will achieve something, but it will be a bare minimum and it will have a lot more room in it to include things like privacy. One reason is that the EU will be in those negotiations and will be pushing its model—and so will China—and I think we will see greater latitude in the establishment of multilateral rules, which the UK will join on to.

Q77 **Martin Vickers:** We have talked about the US and you mentioned Australia, New Zealand and the like. Do you find that the approach in the Japanese agreement will have wider approval? Is this an approach that will find favour with other nations?

Professor Collins: Yes, I think so. Again, I don't want to say that it is identical to what you see in the digital trade chapter of the CPTPP, but it is pretty close. The differences are small and the fact that New Zealand and Australia and so on have agreed to those provisions in that instrument suggests that this is the kind of thing they are comfortable with. We may be coming to the CPTPP, but there are parameters in the CPTPP to pull back a bit through side letters and slightly modify the obligations. That might be where some of these issues get played out.

Martin Vickers: Thank you. Would either of the other two witnesses like to come in on that? No. I have put them into silence.

Chair: Excellent. Silence is golden, as they say sometimes. Turning to a man who is seldom silent, the great Mark Menzies.

Q78 **Mark Menzies:** Someone who is never silent. Professor Collins, how are data privacy issues addressed at CPTPP?

Professor Collins: As I said earlier, the CPTPP is very similar to CEPA in the e-commerce chapter. You have the same recognition of privacy as an important economic and social objective, a requirement to adopt or maintain a legal framework, the same language about ways of complying with this, including the voluntary undertaking. You see a general exception provision, the same language as GATS.

I mentioned earlier that there is a slight difference if you look at the prohibitions on data localisation, which you find in Article 14.13. We talked about the exception for public policy in that requirement. There is an extra sentence in the CPTPP that does not appear in CEPA. There is the requirement that if you enact such a public policy measure that violates the data localisation requirement, or the data transfer requirement as well, it must also not impose restrictions that are greater than required to achieve the objective. That might not seem like much. It might almost seem like it was thrown in there by accident, or someone forgot to erase it, but I don't think so. I think that places an even higher burden on the party attempting to use privacy as a justification, because it expressly emphasises that there cannot be a less trade-restrictive way

of doing it because if there is, it will not pass the test. You have very narrow exceptions to those two provisions.

That is really it. Other than that, I think they are broadly similar. On digital trade generally, the CEPA is a little more modern because it talks about algorithms and things like that.

Q79 **Mark Menzies:** Kristina, to obtain a data adequacy decision from the EU as a CPTPP member, Japan has implemented supplementary rules that treat EU data differently from non-EU data. Is it likely that the UK will have to do the same if it joins the CPTPP?

Dr Irion: To grant an adequacy decision, the GDPR also requires that there are restrictions on onward transfer imposed on the third country that receives an adequacy decision to avoid personal data continuing to travel to jurisdictions with no adequacy decision, for example. It is true that, when Japan was granted its adequacy decision, such a restriction on onward transfer was included for personal data originating in the EU. The reason why this was introduced was, by the way, not about membership of Japan in the CPTPP, but because Japan is also a member of the APEC cross-border privacy rules. It was meant to limit the effect of the APEC cross-border privacy rules, which are based on voluntary standards.

At the moment, until today, there is no EU adequacy decision, but there are not so many anyway. That recognises the role of trade law. However, I believe this will change imminently, simply because we are seeing how much trade law is trying to take over the sphere of governing cross-border data flows. I am not sure if it will change the moment UK gets its adequacy decision, but I saw a resolution by the European Parliament in which there was special mention made to also pay attention to the trade law commitments that the UK has entered into on data privacy, so it is increasingly on the map.

Mark Menzies: Thank you to you both.

Chair: To bring this panel to an end is a former Minister and a man who will give us a great demonstration of brevity, as we are just over the hour.

Q80 **Mark Garnier:** I will be very brief. Kristina, following on from that last question, does the UK Government's strategy of joining CPTPP mean they risk losing their data adequacy decision from the EU?

Dr Irion: I like your question, but it is not a good question. I think the better question would be: how can the UK ensure internal consistency between its own data protection law, at the moment, and its international trade law commitments? It simply seems not very wise to deviate between the two, but for the UK to create a strategy where internal UK law and international trade law commitments converge and are not creating a conflict. Otherwise, there is trouble ahead on one of the two fronts.

Mark Garnier: That is brilliant. Thank you. Very nicely dodged. You have obviously been spending too much time talking to politicians.

Chair: Are we happy with that? We don't want to go to anybody else?

Mark Garnier: Unless Chris or David want to add anything.

Professor Kuner: I will add very briefly that I agree completely with what Professor Irion said. This would really be a way for the UK to be a leader, because to my knowledge there is no country that has tried to produce an integrated approach to protecting privacy in both trade law and data privacy law. If you were to do this, it would be quite innovative, quite powerful and would probably be emulated.

Chair: Excellent. Thank you. We are done with panel 1. Thank you all very much, Professor Irion, Professor Kuner and Professor Collins, for coming along today. I hope you enjoyed it. We are very grateful to you all for coming and sharing your expertise in this quite technical, perhaps niche, but vital area for the flow of trade agreements. The point of that tension between data and trade was probably best teased out during the answer to Lloyd Russell-Moyle's question.