HOUSE OF LORDS

European Affairs Committee

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

Tuesday 30 April 2024

4.10 pm

Watch the meeting

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

Evidence Session No. 4 Heard in Public Questions 35 - 49

Witnesses

I: Martin Kelly, Former Official, Home Office; Dr Nora Ni Loideain, Director, Information Law and Policy Centre, Institute of Advanced Legal Studies, University of London.

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

Martin Kelly and Dr Nora Ni Loideain.

Q35 **The Chair:** Welcome to a session of the European Affairs Committee of the House of Lords pursuing our inquiry into data adequacy and the implications for UK-EU relations. We are delighted to have two very distinguished witnesses today on the law enforcement aspects of data adequacy. I will leave you to introduce yourselves and your careers. Dr Ni Loideain and Martin Kelly, you are very welcome indeed to the committee.

As I usually say, you do not both have to answer every question, because I am sure there will be a range of questions and you can choose which question you would like to major on. We are delighted to hear from you across the range of issues.

To kick off, let me start with a broad question to get things started in addition to you introducing yourselves. Dr Ni Loideain will remember that in 2021 we did an inquiry in the EU Security and Justice Sub-Committee into the law enforcement and security co-operation at that point, as Brexit was coming in, as it were. I wonder how you now see the arrangements in Part 3 of the trade and co-operation agreement relating to law enforcement. How are they operating, three years or so into the practice of them? How much do you think things have changed from what they were before as a result of the new arrangements? It is a broad question; we will pick up a lot of the detail as we go.

Dr Nora Ni Loideain: It is wonderful to be here today. I will briefly introduce myself. I am Director of the Information Law and Policy Centre at the Institute of Advanced Legal Studies at the University of London. I am also an adviser to the Home Office on the independent Biometrics and Forensics Ethics Group.

It is a very challenging task to assess the progress from when the trade and co-operation agreement was first adopted. There is not a very detailed oversight framework for where statistics, for instance, and international exchange, regarding the different mechanisms under Part 3 of the TCA, are operating.

One such gap that has been highlighted by the Office of the Biometrics and Surveillance Camera Commissioner which is due to be abolished under the Data Protection and Digital Information Bill, which is expected to be enacted later this year. The previous Commissioner, Fraser Sampson, has made the point that, while he will publish statistics regarding the existing Prüm framework, the frameworks under Part 3 of the TCA operate separately. He has expressed some serious concerns regarding how the exchange of data between EU bodies and even bilaterally (between the UK and individual Member States) will be covered in future following the abolition of his office. That is my first point: that there is currently an oversight gap in terms of assessing specific statistics

on the international exchange of data from systems for law enforcement purposes.

It would be very fortuitous if the committee could speak directly to individuals within the Home Office, the National Crime Agency and other related agencies to ask what the difficulties have been for police forces, specifically in terms of access to Interpol and previous systems such as SIS II, and the differences there. Because of the lack of independent oversight and scrutiny under the TCA provisions, you have a very narrow set of outcomes and reporting that come from the relevant Specialised Committee for Part 3.

Each of the different parts of the TCA, as I am sure you know, have different specialised committees. The minutes of the meetings of the law enforcement and judicial co-operation committee, which meets annually, are notably brief. In effect, they are highlights of matters that it has discussed. Very little detail is provided in these public reports regarding how systems and data exchange under Part 3 are operating in practice and their compliance with the legal requirements of the TCA.

There could have been another mechanism under the trade and co-operation agreement, under the Civil Society Forum, to have engaged in much more scrutiny of Part 3, but under the TCA the Civil Society Forum was explicitly excluded from reviewing and assessing any matters arising from Part 3. As a result, it is quite significantly difficult, for regulators, policymakers, other affected stakeholders, and the wider public, to assess what the impact has been to date.

Logistically, this is a framework that has been in place for only a very short time. It is quite difficult to assess comprehensively what the impact has been to date, but there must surely be annual statistics from various police forces and agencies as to how the data exchange has been operating.

Martin Kelly: As a quick introduction, I now work as a barrister for Mastercard, but I am not here in that capacity. Previously, I was head of data protection policy at the Home Office, so I was involved in the law enforcement and national security aspects of the Data Protection Bill when that was passing. During Brexit, I was part of the UK delegation that helped to conclude the adequacy decision, as well as some of the data protection elements of the trade and co-operation agreement.

In terms of how the agreement is working in practice, yes, there is certainly limited statistical evidence at the moment. It is still fairly new. We are not too far in, so I hope that will change as things progress. We have so far had three specialised committee meetings on the law enforcement aspects of the agreement and three conclusions that it is operating effectively, so at a high level that seems to be the case.

On top of that, in support of the fact that it is operating effectively, if it was not we would probably see more meetings to try to rectify that, because the agreement works on a "no surprises" principle. If the

Commission or the UK have concerns, they should be raised. You would expect to have seen a further meeting earlier this year if there were currently issues. We will see one later this year.

My third point on this is once again a fairly high-level point. If there were concerns, I think that in the responses in the European Parliament report from November we would have seen issues being raised in terms of how it is currently working. Likewise, I am conscious that the LIBE committee, the European Parliament's committee that would be responsible for this area, has written to this committee and its focus has been on future aspects rather than existing ones. Once again, if there were concerns about how it is currently working, I would have expected to see those being raised at that point.

The Chair: Is it possible yet to draw any conclusions about how our experience as a new third country that used to be a member of the EU compares with those of other third countries in their law enforcement co-operation with the EU, or would we still be short of the data to make that kind of judgment?

Dr Nora Ni Loideain: Could I follow up very quickly on a point that Martin raised regarding the finding from the specialised committee that things are going smoothly overall? I am conscious of stressing that this is all internal scrutiny. There is no external scrutiny from anyone outside these public authorities. Given that the public minutes reported from these meetings are so exceedingly brief, one should invariably be asking questions about how we can be assured (without any supporting evidence for these claims) that the operation of Part 3 is in fact operating smoothly and free-flowingly.

Having said that, I would highlight that there is an ongoing issue that the specialised committee has noted over its three meetings. This is with regard to the retention of passenger name record data. Perhaps the committee will have the opportunity to speak to somebody from the Home Office who could update the committee on this, because the last published minutes came from June 2023, but they were not published until December 2023, so much could have happened in the interim.

However, the EU representatives have been pressing the UK for an assurance that there would be compatibility under the TCA Part 3 regarding our PNR retention regime. Based on the last report that it published, the UK was not in compliance with the passenger name record retention period. We currently have a system that permits five years of data retention and that is far beyond what is currently permitted under EU law, because we had a major Court of Justice of the EU ruling in 2022 (C-817/19, *Ligue des droits humains*) that limited the retention of passenger name record data for countering serious crime and terrorism related to travel to six months. The UK legal regime still permits five years under the 2018 PNR regulations (SI 2018/598), and the UK is on its last extension in the report to address these specific compliance

issues. It has been explicitly stated that no more extensions will be granted, and the deadline was January this year.

It would be very interesting for this committee to follow up to verify whether the UK has met this particular deadline or whether the UK is still in non-compliance with the TCA and the passenger name record retention. There are other issues that are related to non-compliance with the case law of the Court of Justice, but I wanted to highlight that point specifically in relation to Part 3 of the TCA.

Back to your question, I stress that it is quite difficult to make a direct comparison between the relationship that the EU has with other third countries and the relationship it has with the UK, because we have such a unique relationship with the EU. We are a former member state, we are very closely aligned in terms of our legal frameworks generally, and we are a member of the Council of Europe and a Contracting State of the European Convention on Human Rights (ECHR). Consequently, it is quite difficult to make any direct comparisons with third countries that the EU has other legal relationships with which do not have these shared fundamental legal standards.

Q36 **Baroness Lawlor:** On the passenger name retention, what is the basis for applying? How does it work procedurally? Is it open access, the six months versus five years, or does one have to apply? Does one of the parties have to apply for access to the passenger record?

Dr Nora Ni Loideain: When we were a member of the European Union, we implemented a directive on passenger name data retention, which requires that there is mandatory retention by airlines regarding passenger name record data. There can be an exchange of that data between us and other member states.

Baroness Lawlor: Is that on application?

Dr Nora Ni Loideain: Yes. I hope that helps.

Martin Kelly: Yes, it is collected and retained by the passenger information unit, which within the United Kingdom would be the National Border Targeting Centre.

Baroness Lawlor: In your view, is there a good reason for five years as distinct from six months?

Martin Kelly: Yes. There is a law enforcement consideration for holding the data for that long. It was something that was carefully considered when that retention period was concluded. As you have correctly heard, now that we are outside the EU we have to comply with the European case law for third countries, which means that we have to look to delete that data at the point that the passenger leaves the United Kingdom.

There is always going to be a depleting usefulness of the data, but there were operational considerations given as to why the data may be useful

for a period of five years. The longer you hold it, the more you can tell through trends, and it helps in terms of developing rules-based targeting.

Q37 **Lord Jackson of Peterborough:** This is just a quick supplementary to the Chair's question. Europe is an airline hub and a travel hub. How does it work for very close third countries such as Switzerland, Turkey or Norway? What is the experience of those countries? I accept that they are not analogous to the UK.

My other question is about the United States and other Five Eyes countries, such as Canada. How is the EU able to enforce that with a big country such as the United States, which is, I understand, likely to want to keep that data for significantly more than six months? How does the EU reconcile the court decision with that practicality?

The Chair: Could you be fairly brief, because we need to get on to lots of other issues?

Dr Nora Ni Loideain: This touches on some very significant case law that the court has delivered with regards specifically to data adequacy and the test that those standards be essentially equivalent between the EU and another third country. The standards do not have to be exactly identical, but it is the identification of what those standards then should be. As the committee noted in its report from the previous committee meeting on this, "equivalent" does not require that it needs to be identical.

It is an assessment done on a case-by-case basis with different third countries. There is a separate data adequacy framework between the US and the EU, but it is the third one now and there have been difficulties before. The previous two have been struck down by the Court of Justice in the *Schrems* and *Schrem II* judgments, so this is very much an ongoing area of interest. It is expected by some that the current data adequacy arrangement between the US and the EU may well be struck down again, following a pending challenge to the Court of Justice (EU-US Data Privacy Framework). It is a situation whereby the assessment that the UK will be subject to by the European Commission will be different, in terms of our specific legal system and the US's specific legal system.

Q38 **Baroness Blackstone:** Can you tell us about the EU rules set out in the GDPR and the law enforcement directive? We would like to hear what role they are playing in underpinning the exchange of data under Part 3 of the TCA.

Martin Kelly: They are essential. In effect, they provide the rails for the tools to ride along. If you think, for instance, about any international law enforcement co-operation, take any aspect of that and boil it down to its bones, you will see that they all require transfers of data. It is all about exchange of data, whichever relationship you are looking at. In both the EU and the UK, the way of maintaining the right standard is through the data protection legislation, which in my view is exactly the correct way of approaching it. That is what the data protection laws, whether the GDPR, the law enforcement directive or the UK equivalents, are there to do.

In essence, the European data protection legislation and the UK's data protection legislation do two things. First, they protect the data. That is the element that is often considered. Secondly, on top of that, they encourage the free movement of data. To give a law enforcement example of how that can work in practice, take passenger name records, for instance, where you have the National Border Targeting Centre in the UK wanting access to a French airline's passenger name records. The French airline will be holding that data to a GDPR standard. It will not want to release that data to a third party unless that third party is meeting similar standards to it.

That makes complete sense, because there is no point in holding data to a high standard if you are then sharing it with someone who is holding it to a lower standard. That is where the data protection legislation comes into effect, in terms of ensuring that the TCA works in practice.

Baroness Blackstone: Can the UK, at present, access sufficient data from the EU law enforcement system?

Martin Kelly: Do you mean passenger name records?

Baroness Blackstone: Not specifically—across the board.

Martin Kelly: As far as I am aware, it can. That is something that someone who is currently working in law enforcement would need to answer in more detail. Certainly, the law enforcement tools that were negotiated as part of the Brexit deal and that appear in Part 3 were geared towards making sure that we have sufficient access. That is not to say that it is the same access as we had when we were part of the EU. There will be some limitations as a result of Brexit.

Baroness Blackstone: If there is some loss of access since Brexit, does that create any problems for the UK in this area? If we have less than we had before, what are the implications of that?

Martin Kelly: We will probably come on to the loss of SIS II.

The Chair: We are going to come on to that next, yes. Shall we make a transition to that, because that is absolutely relevant to Baroness Blackstone's question?

Q39 **Baroness Ashton of Upholland:** The figures I have in front of me say that in 2019 the police conducted more than 600 million real-time checks via SIS II, Schengen Information System II, which is 1.5 million checks per day. I am not sure I am looking forward to the answer to this, but do you think the post-Brexit arrangements have replaced SIS II adequately?

Martin Kelly: Not like for like. I do not think that is the case. If you were to ask any law enforcement officer whether they would like access to SIS II again, I am sure they would give a definite yes to that.

The Brexit negotiations and the continued discussions following Brexit have tried to limit the gap between the loss of SIS II and the current

position. That is largely done through relationships with Interpol. Work had been done ahead of Brexit to try to ensure an automated supply of Interpol circulations, which gives faster access to information. That is not the same as SIS II, but it helps to limit the impact.

It is different information from what you would find within SIS II. My understanding is that the Government and the Home Office are still working on developing that even further—for instance, getting instant access to Interpol databases, which will help in that as well.

Dr Nora Ni Loideain: To follow up on that, if you are considering this in terms of the pre-Brexit access that we had to data from other member states' law enforcement authorities and where we are now, previously we had the Prüm framework, which we are still a part of, but now Prüm II has been radically reformed within the EU. The EU have a new regulation. It has now been adopted and will become law later this year.

Not only will it cover the exchange of extended categories of data, including facial images and other data that law enforcement would be looking for—expanding the remit of the previous Prüm framework, which is vastly outdated, dating back to 2005 Prum Agreement and the relevant Council framework decisions in 2008—but it will streamline the process by which that data can be accessed, because there will be more of a centralised system now. This refers back to the point that Martin was making about having closer co-operation with Europol, because Europol now will be a hub of data access, in terms of being able to search those systems of member states.

If you were to say to anyone in a police force or a law enforcement authority here, "Would you also like access to the Prüm II system when it comes into being?", I imagine they would emphatically say yes to that as well. Whether or not this committee would make the same finding as the previous committee report about there being an operational downgrade based purely on our pre-Brexit and post-Brexit positions, I would be very surprised at any law enforcement authority that is happier that we are no longer part of the EU and no longer have access to those same systems, especially ones that are developing at the rate at which Prüm II will now be developed in future following the adoption of this new law.

Q40 **The Chair:** A great concern at the time of our report three years ago was that we would no longer have access to SIS II, as Baroness Ashton says, and the alternative Interpol I-24/7 system required EU law enforcement personnel to double-key. In other words, they type into SIS II for the EU member states, but they then also have to type it into Interpol to get it to the Brits. There was a question of whether people would be willing to go on doing that. Is there any data yet as to whether we are getting what we would expect to have got through SIS II because people are still willing to double-key it into the Interpol system? Perhaps the data is not there.

Dr Nora Ni Loideain: I am not aware of any specific statistics that would break down those numbers, but I have been informed about there

now being delays with regard to the system that UK law enforecement authorities would have had used previously and the new system that relies on Interpol. Those delays would not have been there to the same extent before. I think it would be very helpful for the committee to ask someone from the National Crime Agency, for instance, or the Metropolitan Police Service what sort of statistics are available for making those comparisons.

The Chair: That is a good prompt. We shall hope to have a Home Office Minister at the end of the inquiry to wrap it up for us. These are certainly questions we should put to the Home Office Minister.

Q41 **Baroness Ludford:** To what extent do you think the handling of data by UK law enforcement authorities continues to be fully in line with the EU and TCA requirements?

Dr Nora Ni Loideain: To answer your question at quite a high level at first, for the TCA Part 3 it is underpinned by a commitment by both parties, the UK and the EU, that there will be a high level of data protection underpinning this data processing and these data transfers. The use of facial recognition and live facial recognition is a very specific area of concern where we are currently diverging from EU standards and standards of the ECHR in our regulation and governance of a particular police power.

This is particularly acute now because we have had a judgment by the European Court of Human Rights, *Glukhin v Russia*, delivered in 2023. There, the European Court of Human Rights was quite specific about the fact that, when it found the Russian Government in violation of Article 8 ECHR, it was lacking clear and precise rules around when live facial recognition can be used by public authorities in the Russian legal framework.

Here, we have quite a general patchwork of laws that govern not just our use for law enforcement purposes of facial recognition and live facial recognition but emerging AI-based biometric systems more broadly. The former Biometrics and Surveillance Camera Commissioner has also highlighted this point in his annual reports, as did the previous commissioner.

There are certainly issues that would be reviewed by the European Commission in terms of whether, for instance, particular legal frameworks that are governing emerging technologies, such as AI-based systems, are at all diverging from ECHR standards, which we are very firmly committed to, that underpin Part 3 of the TCA, and whether that could jeopardise our adequacy agreement under the GDPR and the Law Enforcement Directive (LED). Facial recognition and AI-based biometric systems is just one particular area where there is generally a consensus that UK law is outdated and falling short of ECHR standards, particularly concerning the right to privacy and also data protection.

Baroness Ludford: You mentioned the discrepancy in PNR retention

periods as well. That is maybe another area of divergence. Mr Kelly, can you think of any plans by the UK Government that would weaken current protections for data and human rights in the UK such as to place the operation of Part 3 of the TCA in jeopardy?

Martin Kelly: I certainly cannot speak on behalf of the Government and potential future proposals, but overall I think that the current regime is safe. That is my personal view on the matter. To go back to the positions I outlined before, the agreement is based on a "no surprises" principle. If there were concerns about how that is currently working, I would expect them to be brought out through the regular discussions at the specialised committee, but also through ad hoc discussions that still take place between officials of the EU and the UK. As a member of the public looking into it, there is nothing to suggest that is the case.

I completely agree with Nora that we have to make sure we maintain our standards when it comes to, for instance, human rights. We have strong human rights in the UK. That is borne out through the limited number of cases that are actually taken against the UK, which is consistent and considerably lower than, for instance, EU member states. We cannot take our foot off the gas when it comes to maintaining those high standards. The UK needs to keep them in mind.

I hear from UK officials that when they are developing, for instance, the new data protection legislation, an important factor they have in mind throughout the development of the proposals, as I did when I was working in data protection policy within government, is the potential impact on adequacy. All the proposals that are being developed have been developed with that in mind. The reassurances from the Government are that they are consistent with the adequacy arrangements we have in place, and I would expect that to be the case.

Dr Nora Ni Loideain: To follow up on that, I would like to emphasise Martin's point that what is underpinning compliance with Part 3 of the TCA is the fact that we have been granted these adequacy decisions, which are the most optimal lawful grounds for processing that we can rely on. There are others, but these enable the greatest free flow of data between the UK and the EU.

Looking at the Data Protection and Digital Information Bill and what has been proposed under that piece of legislation, the European data protection supervisor will advise the Commission on changes in UK law, particularly UK data protection law, and whether there has been any divergence from the time before, when we were granted adequacy.

There will be some red flags. There are a number of changes, and maybe I could focus specifically on the law enforcement context, because I know the Bill has previously been discussed more generally before this committee. There are proposed changes under the draft legislation whereby law enforcement will no longer have to include, in any logs and records that are kept when it uses an automated system, the justification

for accessing or disclosing information from that system. That is quite a significant divergence from the law enforcement directive. It is very black and white.

Another example is the fact that we will no longer have data protection impact assessments. We are going to have risk assessments. I give that particular example because, on the one hand, you could argue that we still have risk assessments—a rose by any other name—but actually it goes a lot deeper than that. Within that particular clause of the new Bill, there will no longer be a requirement to have data protection impact assessments in relation to access by law enforcement authorities to personal data. This is mainly underpinned by the fact that the UK is no longer pursuing a rights-based data protection framework. That is a very clear divergence from the EU data protection framework.

Now, when you have a risk assessment for any such system that poses a high risk to individuals, it no longer explicitly requires law enforcement authorities to address the impacts on their rights or freedoms. It is just a general risk assessment. I give those specific examples to put some flesh on the bones of the fact that we are beginning to show some clear, specific, concrete divergences in how we govern and regulate our law enforcement data-driven systems, and how those standards compare with the GDPR and the Law Enforcement Directive.

There are a number of areas that will be flagged in the European Commission's review of the Data Protection and Digital Information Bill in its assessment of the UK-EU data protection adequacy decisions. There is also the abolition of the Office of the Biometrics and Surveillance Camera Commissioner, the Home Office's justification for that being that it will make the oversight and supervisory landscape simpler. If anything, when you look at the different roles and responsibilities that will then be redistributed to two or maybe more regulators—the Information Commissioner's Office, the Investigatory Powers Commissioner's Office and possibly the Forensic Science Regulator's Office—this is a much more complicated arrangement than before. From a rule of law perspective, it is difficult to see how that is a better arrangement for independent oversight, particularly because it is overloading the Information Commissioner's Office with more law enforcement supervision tasks than it currently has.

There are also issues under the Data Protection and Digital Information Bill with how the Bill proposes to impinge upon the independence of the Information Commissioner's Office. The Bill explicitly requires, if passed in its current form, that the Information Commissioner's Office should start taking into account areas outside of the office's remit in terms of innovation, business and commerce, and that it should take into account priorities set by the Secretary of State.

That clashes, clearly and directly, with the requirement under EU data protection law and in Article 8 of the EU Charter of Fundamental Rights for complete independence for supervisory authorities, and specific

requirements in the GDPR and the Law Enforcement Directive that the supervisory authorities exercise complete independence in their functions and operation. There are some red flags here that did not exist the last time the UK was granted these adequacy decisions, in the form of this legislation, which is expected to be enacted this year and will then form part of the European Commission's assessment for the sunset clause for next year.

The Chair: We were talking about that to the Information Commissioner himself last week, so we are conscious of his views as well.

Q42 **Baroness Lawlor:** Mr Kelly, Dr Ni Loideain has spoken quite well and comprehensively about the problems that could arise from these divergences and the replacement of a rights-based approach with a general risk assessment. Can you take us through, very briefly, the Home Office's thinking on the advantages of divergence and where we see things going?

Martin Kelly: Once again, I cannot speak on behalf of the Home Office, but from experience, I think the objective is to simplify rather than to necessarily diverge from the core principles. Absolutely, I agree that the European Commission will ask questions on the updates to the data protection legislation, and so it should. Whenever there is going to be an update to UK data protection legislation, the EU not only can but should question how that works in practice, because it is an important aspect of maintaining the UK's data adequacy. The UK Government will be expected to address each of those points in turn to explain exactly how they meet the data protection requirements, which are essentially equivalent. We do not have to have the same legislation.

I know that this committee has heard previously from Mr Jones on this issue: how we are starting from having the same legislation and diverging, unlike other adequate countries, which are starting from a point of divergence and trying to approach similarity. There is still an aspect of maintaining standards rather than maintaining exactly the same standards. It will be for the Government to justify that, which, personally, I think they will be able to. I imagine that they are already having conversations with the European Commission on that.

Q43 **Baroness Anelay of St Johns:** Thank you to our witnesses for giving some really hard information about how a system of data adequacy is working now. Some red flags and divergences have been referred to and, as a result, I would like to ask how high the risks are, in your view, of the UK perhaps losing its adequacy under the law enforcement directive. What is your view on that—good, bad, indifferent—and why?

Dr Nora Ni Loideain: I will begin by saying that the TCA Part 3 depends very much on the UK having those adequacy agreements in place. There was a presumption before they were even granted the adequacy agreements that it was inevitable that the UK would be assessed as adequate because we were previously a member state of the EU, with very similar standards, requirements and safeguards in place. It was an

area that was more scrutinised than perhaps some others in terms of data adequacy between the EU and other third countries, because the UK is the only third country that has also been granted data adequacy under the Law Enforcement Directive.

It is perhaps no surprise that that was the case, given our previous membership of the EU, but it could be a cause for concern that that makes us somewhat of an outlier in data adequacy terms compared to other third countries and the EU. If the European Commission decided to take a more sectoral approach to its adequacy assessments, it could find that there were essentially equivalent standards for the GDPR adequacy decision to stay in place, but not the Law Enforcement Directive adequacy decision. That is very much a possibility.

We hope that would not happen, because this is not a time when we would want to see data flows between law enforcement authorities in the EU and the UK hampered or hindered in any way. However, it would be misleading for me to say that there are not some causes for concern, given the above problematic proposals in the forthcoming Data Protection and Digital Information Bill. Also, data adequacy is assessed incredibly broadly; it is the entire legal system, not just our data protection legislation. It is not just the Data Protection Act of 2018 and how it is amended, along with related data protection law. It would also take into account other areas of law that have been questionable in terms of rule of law compliance—for instance, the Rwanda Safety Bill, soon to be enacted. It could also take into account that the UK are soon to become an international outlier in the principles-based approach we have to emerging technologies such as AI, as opposed to engaging with any policy or development in regulating AI. That can be compared as diverging from the approach of the EU, which has adopted the EU AI Act, and there are other related policy developments.

I would not say that there is no risk that we could lose these adequacy decisions. It would be interesting for anyone to say that there would not be any risks, given our current framework and particularly the proposals being put forward under the Data Protection and Digital Information Bill, some of which diverge quite significantly from EU data protection law standards. Even if we are not held to the threshold of having identical standards, the 'essentially equivalent' standard, especially the related safeguards set by the Court of Justice of the EU, are still considered to be quite strict and quite high.

Baroness Anelay of St Johns: I wonder whether Mr Kelly would like to add his idea about the possible level of risk with regard to adequacy continuing under the law enforcement directive itself.

Martin Kelly: As I say, I was involved in the adequacy discussions. To give a bit of context to those discussions, prior to their beginning there were more than 360 pages of documentary evidence provided to the European Commission. During the adequacy discussions, we had 15 rounds of discussions with the Commission, which went into great detail.

Overall, we had more than 1,000 questions asked, both orally and in writing, throughout that period. When it came to its decision, it was based on considerable evidence and testing of the UK's system. It was really important that it did that. We knew we would have to go through that, so that the European Commission could justify the position it took to the European Parliament and the European Council, and it is right that it did that.

Any additional updates since then will obviously have to be taken into consideration. That includes, specifically, the updates to the UK's data protection legislation. I personally think that they still do meet the standards. I would be surprised if the European Commission found that they do not. I would be surprised if conversations are not already happening. It was always accepted, throughout the adequacy discussion process, that over time there would be some divergence. There is no problem with that.

I do not think that there is any problem, because data protection legislation has to develop and we are no longer part of the EU. Naturally, there will be some divergence over time. As I said before, it is absolutely right that the European Commission holds us to account on how our standards meet the essentially equivalent standards of the EU. That will take place through the conversations and the specialised committees, and I imagine it already is happening.

Q44 **Lord Jackson of Peterborough:** May I challenge you a little bit on this idea that the UK is an outlier? Surely, it is an evolving regime in terms of regulation and law. There are plenty of jurisdictions that have a more liberal and permissive approach, rather than a rights-based approach, but we do not know that because it is evolving very quickly. That is an observation.

My question follows from the specific issue that was raised earlier. Article 693 of the TCA talks about a serious and systemic deficiency in one side or the other's policy. What would that look like? What would have to happen for that to be invoked? It seems to me, on the basis of no surprises, that if you have an impact assessment in primary legislation and a proper process through two Chambers et cetera, that is not really a surprise. Therefore, there are opportunities to engage. What would have to happen for the EU to say, "This is in breach of the TCA in this respect"?

Dr Nora Ni Loideain: Given that Martin was involved in the drafting of the text, he may be able to shed some light as to what the drafters had in mind.

Martin Kelly: I am not sure that I have any specific insight into that, although I would say that the two important elements of that are "serious" and "systemic". It would have to be something that would have significant ramifications. That is where the discussions would come in between the European Commission and the UK Government.

To take, for example, the use of data protection impact assessments, would the UK's amendments within its updates to the legislation be a serious change to the legislation? The UK would probably say no. It is a change. It is adding flexibility to the way those obligations can be met. At the same time, the data controller—in this case, the law enforcement organisation— would have to be able to demonstrate that it still meets the requirements of the relevant considerations ahead of processing that personal data. That is the type of conversation I would expect to be happening with the European Commission, asking that question, "How do you still meet those standards? How can you demonstrate that we are not having a serious divergence here?" and for the UK to come back with comments like that.

On "systemic", it would have to be something that has not been fixed. The agreement, in fact, Article 693 as well, talks about having a period of three months, so giving notice. Within that time, the parties should be working together to try to fix the problem. My view would be that "systemic" would have to be after that period. There should be a joint approach to try to fix the problem.

The Chair: That is very helpful. Thank you.

Q45 **Baroness Scott of Needham Market:** I can see in the scenario that you have just described that there could be a, probably protracted, set of negotiations, in essence, with one side arguing that there is a problem, the other saying, "No, we are all right", and some coming together. Nora, you talked about more fundamental things around rule of law; you referenced Rwanda and so on. It seems to me that that is not really a matter for negotiation in quite the same way. It is a rather fundamental political disagreement. I wonder whether both of you could say a little bit about how you imagine that that would roll out.

Dr Nora Ni Loideain: If I just refer back to the question raised by Lord Jackson, it is a really excellent one because there is so much ambiguity about what that threshold would actually constitute in terms of the significant implications it has for jeopardising Part 3 of the TCA and, invariably, the adequacy decisions, because you are still dealing with the same assessment of rule of law complications. Arguably, there are much more significant examples. I was talking earlier about changes to logging requirements for law enforcement and data protection impact assessments. These are significant safeguards but they would not be considered core elements of EU data protection law, for instance.

We should bear in mind two things. We should think about the conceptualisation of death by a thousand cuts in terms of all the different changes that have been made to Part 3 of the Data Protection Act 2018 and how they will be reflected in the Data Protection and Digital Information Bill. A much more significant change to EU data protection law currently proposed is redefining the definition of personal data. It has been much narrowed under the proposed legislation. That is a very significant concept that underpins EU data protection law.

Another very significant area of proposed reform under the Bill in terms of personal data is that UK data protection law would narrow it in certain circumstances to the extent that pseudonymised data, for instance, would not be considered to fall within the concept of personal data. Under the EU data protection regime, it does.

Another quite significant divergence is the fact that our data protection supervisory authority would no longer be exercising their functions completely independently. That is a core, fundamental element of EU data protection law, for instance. They are all significant, but they would be considered much more fundamental.

Perhaps an ongoing cause for concern since we were first granted adequacy decisions and the trade and co-operation agreement was adopted was the possibility of the UK leaving the ECHR. We had a Bill of Rights Bill. I know that that has since been withdrawn by the former Minister for Justice, Dominic Raab. I would put forward that leaving the ECHR, or even the possibility of the standards of the ECHR being diluted under a piece of legislation, would fall within the threshold you were talking about, because we are not talking about a surprise. There were a number of legislative proposals.

There still is political pressure from some quarters that the ECHR no longer be part of UK law under the Human Rights Act and that the Human Rights Act be replaced. That would be a very significant divergence from EU law, the rule of law and the EU Charter of Fundamental Rights, for instance, because the ECHR is part of the EU Charter. It provides minimum fundamental human rights standards in EU law, as provided under Article 52(3) of the Charter. Our pulling that linchpin from our legal system could fit the parameters you mentioned earlier.

Lord Jackson of Peterborough: It would be replaced by a Bill of Rights, one assumes. There would not just be a big gap there. The proposal has always been to replace it with something else. That is for a different debate.

The Chair: It is, yes.

Q46 **Baroness Lawlor:** The TCA does not apply to national authorities that have responsibility for safeguarding national security. On what basis is national security data exchanged between the UK and EU member states? Might I add a supplementary to that? How does this compare with exchanges between third countries, such as the US, by each party?

Martin Kelly: National security sits outside the scope of European law. The Council of Europe, though, has Convention 108, which applies to national security. That aspect was considered when developing the UK's intelligence services regime, which can be found in Part 4 of the Data Protection Act.

The transfers take place on a domestic basis, so it will be between the two parties to determine, in light of the domestic legislation, whether that

can take place. For the United Kingdom, it would depend on who is transferring that data. If it is one of the intelligence services, such as MI5, MI6 or GCHQ, that would be done under Part 4 of the Data Protection Act, which applies to the intelligence services. That regime is based primarily on Convention 108 and the updated protocol to that, which was not in force at the time, but at the same time that was considered as part of the development of the legislation. Where the standards were higher under the Data Protection Act 1998, that was also applied.

Under law enforcement, the transfer would take place using Part 3. There are international transfers under each of these provisions. For everywhere else, it would be under Part 2 of the Data Protection Act. Each of those parts has its own national security exemptions as well that can be applied where appropriate. That is how it would work.

Dr Nora Ni Loideain: To add to Martin's overview, which I very much agree with, there is also a supplemental agreement, the security of information agreement, that was adopted at the same time as the TCA. Emphasis really is on "supplemental". It is a nine-page document, compared to the 2,500-page document we have for the TCA.

That agreement permits the exchange of classified information, which is defined very broadly, between the UK and particular EU institutions and bodies. There are provisions within that agreement such that, with prior approval and assurances regarding the confidentiality and safety of that classified information, the EU institutions could share it with other EU institutions and entities. Those entities could include, for instance, Europol.

Baroness Lawlor: Some intelligence academics, I suppose I would call them, have suggested that one has to be very careful about which countries one shares data with. Would you like to comment on any of the potentially hazardous destinations for such security data?

Martin Kelly: I would not name specific countries, but on top of that there is also the human rights legislation that has to be applied. Generally speaking, in terms of national security bodies, whether that is the intelligence services, law enforcement or others, the types of data we are talking about would be sensitive and classified. From the UK perspective, they would be given a recognised security classification. They would want to transfer and share that data only with trusted parties, for obvious reasons. That, in itself, would be an additional protection of the data.

Q47 **The Chair:** May I follow up Baroness Lawlor's question by probing on the issue of onward transmission of EU data to third countries via intelligence or law enforcement channels? That, surely, would be the really difficult problem, if there was a sense that EU data was being shared with the Americans, for example, in a way the EU was not happy with. Should that concern us, or does that also fall outside the scope of Part 3?

Dr Nora Ni Loideain: It would certainly be a matter for the committee to consider. It is a matter of significance, because the LIBE committee and the European Data Protection Supervisor (EDPS) have both said that the UK could be considered as a mechanism by which data such as this might be transferred to third countries that have not been granted data adequacy by the EU or recognised by the EU as meeting its rule of law and human rights standards. I highlight that mainly because it is one of the key concerns raised by the LIBE committee, the European Parliament and the EDPS.

The Chair: Thank you very much. Does anybody have any follow-up questions while we still have a few moments of your time?

Q48 **Baroness Ludford:** Yes, as long as we are beating the bell, I have a question. Did I correctly understand—I think Nora might have said this—that you envisage a scenario where we retain adequacy under the GDPR but lose it for law enforcement? Could you imagine that split?

Dr Nora Ni Loideain: I could imagine the risk of that happening. This is based on the fact that the UK are in a unique position, in that we are the only third country that has been granted adequacy under both those EU laws—the Law Enforcement Directive and the GDPR. That would be based on the European Commission taking a less pragmatic approach and a stricter scrutiny approach that would align much more closely with the Court of Justice's EU case law, for instance, but also taking a more focused sectoral approach to assessing adequacy and essential equivalence and not considering both in their entirety.

There have been some suggestions that the European Commission could be moving in that direction, but I would hope, from the perspective of enabling and ensuring the continuation of data flows between the UK and the EU, that we would not have to face that situation. So much depends on legal developments that will be taking place between now and when the European Commission concludes its assessment before the sunset clause. A significant cause for concern is the Data Protection and Digital Information Bill and the changes proposed under that.

The Chair: There is a last extra-time question from Lord Jay and then we will let you go.

Q49 **Lord Jay of Ewelme:** What would happen if we lost our adequacy arrangement?

The Chair: Would it cut off all co-operation between UK law enforcement and EU law enforcement, which would be a huge setback?

Martin Kelly: No, it would not, not completely. Actually, the way the TCA is drafted, it is not a requirement to have adequacy for the tools to operate. It would become very difficult.

Lord Jay of Ewelme: What would become very difficult?

Martin Kelly: Part 3 would be very difficult if we lost adequacy, but, strictly speaking, technically not impossible, because, the way that the TCA is drafted, it is not a prerequisite to have adequacy. You can imagine, in a situation where we lost adequacy, that that would pose a lot of difficult questions for how Part 3 would continue.

It would depend partly on the reason why we lost adequacy as well and whether it was fundamental across the tools or impacted on specific tools. On top of that, not all of the law enforcement tools—the various tools within Part 3—are dependent, for instance, on law enforcement. If we lost the law enforcement adequacy but not the GDPR, it would be possible, for instance, for passenger name records, not being reliant on the law enforcement adequacy, to continue.

To the Chair's question about whether all law enforcement co-operation would stop, the answer is no. It would still be feasible to operate. The European Union law enforcement agencies have relationships with law enforcement globally and they do that without a law enforcement adequacy decision. The difficulty would be that the amount of information we get and the speed at which we get it would be severely hindered if it was not for the TCA.

Lord Jay of Ewelme: It is not an absolute, in a sense. It is not all or nothing. What the decision not to give it to us is based on would influence what happens afterwards. There are gradations of losing of adequacy.

Martin Kelly: Yes, there are. It is in no one's interest, neither the EU's nor the UK's, for there to be a reduction in co-operation between UK and EU law enforcement. I hope that we would not get into that position. If there was, the UK would have to work with the EU to see how we could continue to co-operate as effectively as possible, but without that adequacy decision.

We would be in a different position, in my view, from a no-deal position—for example, when we were leading up to the end of the Brexit negotiations. We would be in a different position from not being given adequacy in the first place, because there is a difference between not being given adequacy and having adequacy explicitly removed from you. That is a different position, and a harder position to be in. That is another factor that would have to be considered.

The Chair: I am so glad we have been able to get through that without another vote. There was a lot of very useful information for the committee; thank you very much indeed. If anything occurs to you afterwards that you wish you had said but did not have the chance to say, you are very welcome to write to us, and we will take that into account as well in considering our inquiry. Many thanks.