



European Affairs Committee

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

Tuesday 14 May 2024

3 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 Scott of Needham Market; Lord Stirrup.

Evidence Session No. 6

Heard in Public

Questions 62 - 71

Witnesses

I: Robert Jones CBE, National Crime Agency; Peter Ayling, Assistant Chief Constable, National Police Chiefs' Council.

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

Robert Jones and Peter Ayling.

Q62 **The Chair:** Good afternoon and welcome back to the European Affairs Committee of the House of Lords. We are continuing our inquiry into UK-EU data adequacy and its implications for UK-EU relations. I am delighted that we are joined this afternoon by two operational law enforcement people who can guide us through this. We have Robert Jones, the director-general of operations at the National Crime Agency; and Deputy Chief Constable Peter Ayling from the National Police Chiefs' Council. Gentlemen, thank you very much indeed for being with us. We will, in the usual way, produce a transcript and make sure that you have an opportunity to review it before it is published.

Let me start by saying that you should feel free to answer the questions are comfortable with answering. You do not both have to answer every question if you choose not to. Could you set the scene for us by talking about how you see the current arrangements in part 3 of the trade and co-operation agreement? We discussed it in an earlier session of this committee. How is it working in practice? That is what the committee would be most interested to know, I think; we will come on to more detailed issues after.

Robert Jones: I will make some opening comments, then Pete can come in with anything he wants to add from the policing perspective. In terms of setting the scene, the first thing we would say is that, since you heard from us last, we have done a number of things to help take some of the risk out of the proposition of losing access to the SIS II data and extradition—that is, the loss of the EAW and our ability to extradite using the TaCA arrangements.

One of those is the Joint International Crime Centre, which was formed in the National Crime Agency. It is a joint unit with policing and is now up and running with more than 200 officers; it gives the capability to look at data and work bilaterally with policing and police forces in the UK. The other is a national extradition unit, which gives us a national footprint to deal with extradition. Then there are a range of other measures, including Prüm and the ability to get DNA hits with a range of different partners that we have signed up to.

A combination of those things means that, in effect, we have a streamlined TaCA process for extradition, which has worked. We have been able to maintain broadly similar levels of inbound requests. Of course, it is not as slick as the previous arrangements, but, from where we sit, we are able to receive requests, to validate them and to deal with those extraditions in a business-like manner. So we have recovered from the original concerns that we had. We have, in effect, what I would describe as a patchwork of different measures that have been brought together and overlap to create the risk mitigation that we needed to deal with what we lost.

Peter Ayling: I will add a couple of bits if I can. I reflect on the first time that I sat before one of these committees. It was in the immediate aftermath of EU exit. We had gone through a prolonged period of uncertainty and were adjusting to what was widely considered to be a good deal with some notable concerns; I know that we will come on to SIS II.

In the run-up to that and immediately after, there was a real shared sense of joint endeavour throughout UK law enforcement agencies and international partners. I have seen no diminishment of that. Of course, that is really important in terms of practical application and the appetite to continue to exchange data and co-operate in this way.

In the immediate aftermath, the International Crime Coordination Centre undertook a lot of training, development of new policy and monitoring of the use of international tools, as well as developing new capabilities. We started to work with the NCA much more closely. I do not think it is an insignificant achievement that we have now seen that transition into the Joint International Crime Centre, which is an NCA enterprise but is very much a joint unit that leverages the capabilities of the agency with policing and consolidates the benefits that were gained. In many areas, what we can see is the maintenance of the use of tools, the sharing of information and gradual improvement.

It would be remiss of me to say, from a policing perspective, that there are no opportunities for that to improve—particularly in areas that were previously automated—but I am encouraged by the plans for the future. As long as we stay the course, I can see an opportunity to improve on the current arrangements and get back to a level of automation and greater join-up so that we address the issue at the moment, which is that we are getting similar output but the effort and labour to achieve it is greater.

Q63 **The Chair:** Of course, speed can sometimes be of the essence in this world as well. Can I drill down into one issue: the Prüm database? Again, that was an issue, although we judged at the time of the TCA that we maintained essentially the same access as we had had as a member state. Has that proved to be the case in practice?

Robert Jones: It has. It has been very successful. Some 25 out of 27 countries are now active. We regularly exchange material with those countries and the numbers have gone up from around 10 proactive requests leaving in the UK initially to around 70 a week. That is significant.

What does that mean in real terms for public safety? It means that, where a burglary is undetected in the UK, we can disseminate material and there might be a DNA hit. We can then identify the perpetrator and a local force is able to arrest somebody for burglary. We have a similar range of results across crime types, including rape and other serious offences.

So that is a real success and something that we are looking to build on with the other accesses that Prüm will give, which we hope will include vehicle-keeper information and criminal records information in the future. From where I sit, that has been a very successful piece of work.

Peter Ayling: I would echo that. One of the challenges and nuances for international partners as they engage with the UK is that they are somewhat surprised by the patchwork quilt of territorial policing and the myriad forces that need to understand and respond to those requests. Having a central unit in the JICC to co-ordinate that and be a point of authority, guidance and advice is helpful. Prüm has been a real success story for policing, and I am greatly encouraged by how much better sited territorial forces are on the benefits of Prüm. You can see that in terms of its proactive use and you can also see it through the step 3 process that was introduced. Step 1 will be where a hit is notified. Step 2 is where that is then transmitted to the investigating officer to take some action. Step 3 was introduced to understand the "so what?" from that, and the consequent action. We can start to see much greater use, whether it is for intelligence purposes or in judicial processes. We are starting to see much more consistency and uniformity across the many different police forces. So it has been a success.

The Chair: To give a sense of comparison, are the 70 outgoing requests roughly comparable to the pre-Brexit level?

Robert Jones: Prüm developing coincided with exit. There is not really a comparable baseline because this is new capability that we were we were committing to. But we are certainly seeing an increase. We have seen the positive results that we are getting back in terms of identifying suspects, and resolving and detecting crimes that would not have been detected without it.

Peter Ayling: Rob is right. It was early in its implementation. In the run-up there was certainly a level of concern that something we were enthusiastic to contribute to might be lost and at the time we were a volume contributor. Obviously, that has not been the case and we continue to be a volume contributor and make very good use of Prüm.

The Chair: That is very encouraging.

Q64 **Lord Stirrup:** This inquiry is looking at data adequacy arrangements between the UK and the EU, how well they are operating now, and whether they are likely to continue into the future. Clearly, in terms of security and policing, the co-operation arrangements set out under part 3 of the TCA are crucial to ongoing effectiveness. On the other hand, they also seem to be the area that could perhaps put data adequacy agreements most at risk. Can you set out for us your view on the extent to which the EU rules in the GDPR and the law enforcement directive impinge, or might impinge, on the adequacy of policing and security arrangements, and vice versa? How might our interests put at risk continuing agreement on the data adequacy arrangements, in particular,

regarding the European Court of Justice ruling on PNR for example? Six months versus five years is a pretty big gap. Are we likely to resolve that issue? What are the risks to this crucial co-operation in future?

Robert Jones: I will give you an operational perspective. The kind of policy conversations and political dialogue to make sure that what you describe does not happen are not within my gift, I am afraid, but I will give you my perspective on where we are at. The ability to create data and deal with it professionally underpins everything we now do in national security and organised crime. We pay a lot of attention to that.

A lot of the work that was done to make sure that concerns around adequacy or concerns around GDPR had already been done. We take that seriously. We have mandatory training in policing and the NCA, whereby people are expected to be able to be data literate and to deal with data in a professional way. That underpins the adequacy status that we have now.

Certainly, we would be concerned if there were any change to the TCA arrangements or if anything undermined our ability to exchange data. My understanding is that we would still be able to disseminate data, but we would have to have a series of, again, overlapping multiple bilateral arrangements with other partners for them to be able to disseminate data to us. I do not relish the prospect of that as an operational leader. We would obviously want to do everything we can to preserve the current arrangements. As I say, some of the policy considerations around that are outside my ambit.

Peter Ayling: There is not much that I can add from a policing perspective, save to say that data adequacy was enormously beneficial in the seamless transition for us to be able to use international tools under the trade and co-operation agreement. The seamless transition of data and digital communications must be a high priority, and anything that jeopardises that would be unwelcome. However, as Rob has said, we have strong safeguards in the use of personal data. We are subject to scrutiny and inspection, and are answerable to the Information Commissioner's Office.

There are pretty solid guardrails to ensure our adherence to data protection standards. The area of personal interest, and it is not one that has arisen, is where an issue of adequacy might touch on matters of public safety and would seem to trump it. I have not encountered anything in that regard. You would expect my focus to be around domestic legislation and obligations on chief constables to ensure the protection of their communities and people. But I am reassured through dialogue with Home Office partners and existing governance that, should such matters arise, there are methods to ensure their remedy. One of the points we come back to is that it is in our mutual interest to be able to bear down on people that might cause harm and to share data in doing so.

Lord Stirrup: We think about this a great deal, of course, in terms of

information coming from the EU to us and the way in which protect that information. But this is about data exchange. Can you give some sense of the extent to which this is an important two-way flow as opposed to us taking information from EU countries?

Peter Ayling: It is self-evidently important as part of that two-way flow. I have no data that I can draw upon, save to say that with a host of international partners, there is a firm commitment to be able to transact, whether it is investigations, transferring information or Interpol notices—there is a host of examples that you could use to say that there is a reciprocal interest in the free flow of data.

Lord Stirrup: I am just trying to get to the evidence that there is a significant two-way flow. You talked about mutual interest. There is a significant stake that other EU countries have in this as well as ours.

Robert Jones: Absolutely.

The Chair: Is there anything to add on the passenger name record point—the risk that our regime will become increasingly separate from the European one?

Robert Jones: We would be concerned if the impact of those changes was an inability to access PNR data. But the reality is that we rely on other agencies to deal with that data for us. Home Office and Border Force are the lead agencies in dealing with that. The Home Office is responsible for the policy around it. We still we have good access to it through the National Border Targeting Centre. We use it proactively and need it. It is a vital tool for us.

Q65 **Baroness Ashton of Upholland:** I will turn to Schengen and Interpol specifically. In 2019, there were some 600 million checks using SIS, the Schengen Information System II. I am interested to know whether the arrangements that we have had post-Brexit are working well. Specifically, are you getting the same volume of alerts and, through the Interpol system, is this working as well because of the need for double keying, as we call it? The way in which you talked earlier sounded to me like we have systems that work but are a bit clunkier. They take more labour and are less smooth—you put it better than I did. Is it taking longer to upload Interpol notices? Are the things around this that, in an ideal world, you think could be made to work better?

Robert Jones: There is an overall point around digital technology in law enforcement and multi-year investment in technology solutions which allow us to do what we need to do in a digital world. This is one of them.

We need robotic process automation and tooling that pulls through the data in a way that does not require manual intervention. That is something we are trying to develop and have running in the JICC. We need more of that and more sustainable investment to mainstream it.

One of the other things around the SIS II versus Interpol debate in terms of notices is that there is not a like-for-like comparison. With SIS II we

had a lot of automated promiscuous checks, where alerts were generated that were not necessarily targeted by a specific request. We now see an increase of Interpol diffusions with some countries and with others we see less, but the net result of those disseminations, in terms of extradition and criminal intelligence, is a similar response. However, the figures are very difficult to compare because it is such a different animal from SIS II.

It seems that some countries will not double key and will target a request through Interpol channels if it is for the UK and there is a defined criminal intelligence link to the UK. That is how they will get the request to us. Others will double key and do both—in effect, they will spread-bet. There is a mixed economy in terms of use. What matters to us, if there is a criminal in the UK, is that that request is targeted to the UK and, likewise, that we can target outbound requests to the right place.

Peter Ayling: This is a really difficult area. Policing has been on the record from the outset to say that the loss of SIS II represented a significant loss of capability. I have not changed my view in that regard, but a lot of work was done to mitigate the loss of that tool. I will not comment on the external elements, in terms of the use of international partners in raising notices. My big concern in the early days of EU exit was to ensure the knowledge and capability of police forces to continue to triage for an international dimension and raise the relevant alerts.

You described the system as clunky. That is accurate. Something that was seamless and automated now requires somebody to recognise and input information, somebody to receive and raise the notice, and somebody to check for that information at the other end. It is clunky and requires more effort to put in, but a suboptimal system has been made considerably better over time. A simple example is that the ICC developed a smart tool application very early on that removed the chances for errors in inputting information into the International Crime Bureau. The JICC has taken that and moved it on further, so the risk of errors being made has decreased and the speed with which that information can be uploaded has greatly improved.

An important development in the background is the international law enforcement alerts platform, or I-LEAP. I have been closely engaged with that from the outset. It creates the technical architecture to access and share information via Interpol. The first stage has been to sign up all UK police forces and wider law enforcement to I-LEAP. I am pleased to say that programme has advanced very well. We are now at the point that every law enforcement agency has signed up and very soon will be onboarded to the I-LEAP platform. We are seeing consistent rises in the use and checking of information via Interpol notices because that is now directly available through domestic systems to interrogate Interpol find databases. That is a really welcome development.

However, it is important to say that the next two stages are critical if we want to move back towards something akin to SIS II. The first is

integration into LEDS, which will be the replacement for the police national computer. That will mean I-LEAP is part of a federated search, rather than having to search independently on a different system. The third prize is the ability to sign multilateral agreements with EU member states, which will enable the sharing of real-time alerts through I-LEAP. Where we are is a distinct step forward and it has made a clunky process less clunky, but I am really ambitious—and, if I am honest, slightly impatient—to move to the next stages, which are making sure this is integrated with our domestic systems and linking it to multilateral agreements with international partners.

Baroness Ashton of Upholland: When you say “multilateral”, does that mean groups of countries? How do you define it?

Peter Ayling: It is not an area on which I can speak with authority. My understanding is that in I-LEAP’s early stages it was conceived that bilateral arrangements would be agreed with priority countries. I think a directive via the European Commission around law enforcement co-operation hinted that it may be possible to sign an EU-wide multilateral agreement and it was perhaps worth pushing the timescales back to seek that prize. You would then be very close to the situation we had with SIS II. Apologies, I am not the senior responsible officer so I would not want to mislead you to say I was the voice of authority on that.

Baroness Ashton of Upholland: Not at all. I have just one more comment, which is that we make the very difficult job that you do harder. I am sorry about that, because we should be looking at every possibility to make it easier and avoid anything being missed. Presumably, then, if we lost data adequacy, things could only get worse.

Robert Jones: They could. There are a number of ways of exchanging data, though. We made it clear that we do not want the loss of data adequacy—of course we do not—but we would still seek to exchange information bilaterally. It is the basic “adapt and overcome” as these challenges come, because we are in a very different place from where we were.

Peter Ayling: Again, from a policing perspective, it is incredibly challenging to ensure that 43 police forces, large and small, understand the nuances of these issues. Hence the importance of a central and authoritative voice in the Joint International Crime Centre. I think we have the foundations that could cope with that. When you say “get worse”, experience has shown that joint endeavour and pragmatism will prevail; it just requires more heavy lifting. I do not welcome more clunkiness in the system.

Baroness Hayter of Kentish Town: In a way, this is about that clunkiness. You have slightly described it from our point of view. How do your opposite numbers, who have to get used to a change in the system, feel about it? How would they describe their ability to get stuff from us when they have needed it?

Robert Jones: I will give you a perspective in terms of liaison and the multilateral presence we have in Europol, then Pete can come in as well. We are still in Europol; there are still 10 British officers there. Obviously, we are a third country now so it is a different type of arrangement, but we are a very important partner in Europol. Europol wants us there and we work very closely with it. We have just hosted the European police chiefs in the UK. We have a very close and productive relationship with them. Europol wants to access data from the UK and it works very closely with us. We have got to a position where, through both multilateral and bilateral channels, we can and do exchange data. Of course, Europol would prefer that we were not a third country, but we are. We are over that, and we have a productive relationship with it.

Peter Ayling: Rob is a great authority on international matters and the views of international partners. From my perspective, one of the groups we work very closely with is the foreign law enforcement community that works here. That is where I regularly see that joint endeavour and determination that there is no degradation in the way we work together, and a determination that the effort is put in to ensure that is not denuded in any way. I echo the point that they would probably recognise that things were somewhat more straightforward beforehand.

Q66 **Baroness Blackstone:** My question relates a little to the one that Baroness Hayter just put. Can you tell us how far the handling of data by UK law enforcement agencies—presumably that means mainly police forces, but not entirely perhaps—is accepted by the EU and the TCA? Does it meet their requirements? Do you get criticisms sometimes?

Robert Jones: The operational exchange of data for criminal investigations and intelligence purposes is productive on a day-to-day basis. They accept it and will action it. That is done through accredited channels. Currently, there is no challenge to the way in which we handle data in terms of UK law enforcement on a day-to-day basis.

Peter Ayling: There is nothing to add, other than to say that we have talked about the safeguards and guard rails that are in place. It is challenging. You said that volume of transmission is via police forces. It is important to have appointed people and highly prescribed, scrutinised processes to ensure that data protection is managed. I am confident that they are in place.

It seems inevitable that, over time, there will be a need for review and revision, both because of the changing nature of legislation and as issues arise. However, I made this point earlier: I am confident that the governance exists to achieve swift remedy should such concerns arise. In my time in the role, I have not been aware of concerns raised with me expressly about the handling of data by UK police forces.

Q67 **Baroness Blackstone:** You have more or less answered the question that I was going to put, which was about how far you can respond to changes in law enforcement agencies across the EU. They change just as ours change, so it must need quite a lot of attention to take into account

what is happening in the EU generally and in particular countries specifically.

Peter Ayling: That is an issue on which I am probably not the best person to respond, save to say that there is regular dialogue regarding the safeguards that exist in policing and where issues pertain to our ability to carry out our core function. I have not hitherto experienced something that has been so difficult that it cannot be reconciled. Either the provisions are in place, there is flexibility or there is provision that reasonableness and necessity trump what can be prescribed in every circumstance. But I agree with you that it will require ongoing review and vigilance over time.

Baroness Blackstone: Who is having that regular dialogue? That is my last question.

Peter Ayling: From my perspective—as a representative of policing, I sit on a number of international boards—it is probably the International Crime Cooperation Board, chaired by a director in the Home Office, which pulls together many of these issues in to ensure that there is alignment across the wider law enforcement system.

Baroness Scott of Needham Market: I was interested to hear about the meeting in London, our status as a third country and that the relationship is still good. We were not the only third country. Thinking about that, are these arrangements similar for all or is there a patchwork of arrangements between countries? Do any countries have aspects where you think, “It would’ve been really good if we could’ve done that”?

Robert Jones: The strength of the relationship means that, although we are a third country, it is a very strong relationship. I am not aware of a wish list of asks that we have where we think that others are getting more than we are. I cannot speak for those other bilateral relationships but, when we work with our Five Eyes partners and internationally, we are certainly one of the leading countries in terms of engagement in Europol and one of the leading contributors on intelligence. Although we do not lead task forces anymore and cannot lead JITs, we are members of a number of task forces on everything from immigration crime to cyber and drug smuggling. We actively contribute and receive intelligence through those channels. The answer is that I am not aware of a special arrangement that other people have.

Q68 **Baroness Ludford:** Thank you very much for coming, gentlemen. I recall that we once had the directorship of Europol—for a decade, indeed, in Rob Wainwright. I want to ask you about how high you think the risks of the UK losing adequacy under the law enforcement directive are. What are the key factors that could lead to that risk of a loss materialising?

Robert Jones: I can give you only a limited answer to that because I cannot accurately assess that risk. It is a legal position that requires some consideration and advice. What I can say is that, operationally, we are doing everything we can to maintain standards and reduce that risk.

This goes to the points that Pete made about training, curating data professionally, how we exercise data protection in the UK and how we work with the ICO, but I am not really in a position to assess that risk accurately. That is for others.

Baroness Ludford: Okay. I note you said earlier that, for instance, retaining PNR data for five years—as against the EU standard of six months—is a matter of policy and not for you. Can I press you a little on that? It is so important for you, as agencies, to have law enforcement adequacy. Presumably it is not beyond your scope to raise red flags with the Home Office and the Government when you see things that you think increase the risk. I know you say that it is not in your purview—I totally accept that—but it is presumably on your radar to say when you think that something will put your operational capabilities at risk.

Robert Jones: Yes. If we saw scenarios developing where we could see a current and direct threat, we would escalate them through the Home Office and officials. What I am saying is that we do not have a number of concerns that I can give you today saying that that is leading to a big threat to those arrangements. The point about not being able to assess is a point about legal risk. It is a legal framework. It is not for me to assess it—that is for others to do—but I can assure you that, if we identify areas where there is a clear threat to our operational activity, we escalate them.

Peter Ayling: I would reinforce the point that there are strong provisions in place to make sure that standards are maintained. I would not want to be glib and say, “Data adequacy isn’t important and we don’t think it should be safeguarded”. It absolutely is, and we do. The point is that there are mechanisms to raise issues where you think adequacy might be threatened; those can be responded to.

As I said, there is also the potential that safeguarding adequacy at all costs might be seen to trump other issues that would be a priority to me, such as maintaining public safety. There is vigilance on both sides, but I am fairly confident that, through the governance arrangements and extensive dialogue—I think that it is now much more extensive and, in many areas, integrated than was the case before—there is the forum and the opportunity to raise and respond to those concerns.

Baroness Ludford: Given that there are two adequacy decisions—the law enforcement one and the GDPR one—could you envisage a scenario where the UK lost one but not the other? What factors do you think could influence that?

Robert Jones: Again, I can give you an operational perspective on that. The ways in which we handle data and operate on a daily basis are really important. We have developed frameworks that mean we are compliant with the GDPR. Although there is not a direct comparison, on the adequacy provisions and equivalence, we have worked very hard to maintain those standards. That is what we will continue to do. Again, I do

not really want to comment on the likelihood of those two things happening separately and us losing the GDPR, with that being a separate issue from adequacy. That is not something I can really call, I am afraid.

Lord Stirrup: The sense I have from your evidence so far is that, if we were to lose data adequacy with the EU, it would become clunkier but you could work around it—in other words, effectiveness would remain although it might be less efficient. Based on something that Deputy Chief Constable Ayling just said, may I turn the question round? Are there aspects of complying to an extent that maintains data adequacy that weaken our policing or security arrangements? In other words, are there changes that could be made to the regime that would produce a better outcome than we currently have?

Equally, are there risks down the line with what is happening with data protection in the EU that could make our policing and security arrangements more problematic?

Peter Ayling: The short answer to that is: not that I am currently aware of or working on. As an issue that has been discussed, there is potential for tension to arise in the future, whereby data adequacy would seem to take primacy over matters of public safety. I have discussed with others the implications and the extent to which proportionality and necessity are described and are adequate to work within the current agreement. However, it is difficult to comment on what the future will hold, save to say it will undoubtedly change and need constant review and revision. That is where my priorities are: to have confidence in the systems whereby those concerns can be raised and resolved, or at least heard, with international partners with a clear, authoritative voice. Certainly, through the work with Home Office officials, I am confident that that is in place and I do not have any specific concerns that data adequacy currently undermines our law enforcement response to operational matters.

Robert Jones: I agree with that.

Lord Jay of Ewelme: Picking up what you said, deputy chief constable, about taking it up with international partners, if you had the sense that something might happen that was going to be unfortunate and deleterious from our point of view, would you take that up with the Home Office? Would you take that up with international partners? What are the mechanisms for discussing with others something that you feel might be going in the wrong direction?

Peter Ayling: I can answer that from my position as the NPCC lead. We have a number of committees that rise through the Chief Constables' Council. That is one route of escalation. Of course, my work with Rob's teams through the Joint International Crime Centre has an important voice as a single front door for UK law enforcement and international partners. In most instances, that acts as a voice of authority to ensure that there is a shared situational awareness of the issues and can

therefore raise them to the appropriate person. But most of my dealings in terms of this particular issue are with officials within the Home Office and through the International Crime Coordination Centre whereby we are able to bring together law enforcement across the UK more widely and ensure that alignment of interests.

Lord Jay of Ewelme: But are your contacts with your European partners such that if you see something coming up that looks dangerous, you can say, "Look, hang on a bit, we just need to do this in a slightly different way in order to ensure that we have something which is in all our interests"? Can you and do you do that?

Peter Ayling: I do not want to play the same record, but, from my perspective, it is really important that we work now as part of the JIC, because whereas my focus is largely downstream and building capabilities of territorial police forces, Rob's focus through the NCA will be looking upstream. So this is probably best responded to by Rob.

Robert Jones: To add a little to that, we would of course raise it operationally through all our channels. If there was something specific that a partner was pursuing operationally that would lead to an adverse outcome for us, absolutely, we would raise it and escalate it. To achieve a shift in that policy position with their interior ministry would require engagement with the Home Office and FCDO, and potentially political engagement. That is what we are alluding to. However, we will not hesitate to, and we do so regularly, engage with operational partners to say, "It would be really unhelpful if you were to do that". But we could achieve the shift only by going through policy officials in the Home Office and elsewhere.

Q69 **Baroness Anelay of St Johns:** In answering our Chair's question at the beginning, Mr Jones, you referred to the fact that there had been a strong effort to ensure that there was a patchwork of measures that could provide us with security in the way in which we were dealing with criminal matters and exchange of information. Can I take you into a more sensitive area? The TCA does not apply to national authorities tasked with safeguarding national security issues. Are you able to give us your view? On what basis does national security data exchange between us, the UK and EU member states work?

Robert Jones: I am afraid that is not something I could or should answer. That is for elements of the UK intelligence community that deal with that. It would be wrong for me to answer that on their behalf. It is for them to answer.

Baroness Anelay of St Johns: What relationship do you have with them? How does that work?

Robert Jones: We have a good relationship with partners in the UK that deal with counterterrorism and national security, and we exchange data with them. But, of course, there is a range of arrangements for them to

deal with their partners across Europe, and it would be wrong for me to answer on their behalf.

Baroness Anelay of St Johns: I understand. We have heard with interest about the Joint International Crime Centre. Could that also be one of the sources of exchange of information on security matters?

Robert Jones: It could be, depending on the scenario. Typically, there are strong bilateral relationships between the intelligence community in the UK and elsewhere, and they have strong partnerships. However, it may be the case that if an extradition or something operational was overt and required action, the Joint International Crime Centre would be involved. But the range of options available for intelligence transfer is a matter for those agencies.

Baroness Anelay of St Johns: Peter Ayling, are you satisfied that you have a relationship with those who operate in the rather more sensitive world whereby that organisation or organisations are very much aware of information that you may need in advance to be able to do your job properly.

Peter Ayling: Yes, I have a very high level of confidence. The counterterrorism policing network is well embedded with all police forces. That glib phrase, local to global, is a well-established link through all elements of policing. I have a high level of confidence in that regard as it pertains to security.

Baroness Anelay of St Johns: We have already had questions from my colleagues about what happens if we lost data adequacy from the two avenues. Do you see any risk of that happening because of the work that has to be done on security matters, where you may not be necessarily given the information fast enough to be able to give advice?

Peter Ayling: It is not a question that I can answer with any authority, save to say that I am not aware of any issues that would give me that concern.

Q70 **Lord Jackson of Peterborough:** Mr. Ayling, the most striking piece of evidence is the tension that you have referred to between data adequacy and political decisions over that and public safety. I hesitate to ask you to speculate on what may happen, particularly in such a sensitive area. As you know, the European Court has sometimes taken a sensitive approach to, particularly, the onward transfer of data to other partners. Are you and Mr Jones satisfied that, should the court take an absolutist position that undermined the operational efficacy of, for instance, the Five Eyes arrangement, you would have in place mechanisms to make those concerns apparent operationally, politically and at government level?

Peter Ayling: I am very confident that we have a voice and a mechanism to raise concerns. An important point of clarity is, rather than there being tensions that we are responding to, the potential for there to be a tension between adequacy and an issue like public safety are not

concerns that I have and am responding to now. But yes, in terms of being able to spot, raise and have influence on such matters, I am very confident.

Lord Jackson of Peterborough: Do you agree, Mr Jones?

Robert Jones: I do. We have a strong relationship with Five Eyes partners, Europol and others, and Interpol. Through all those channels, we can make those concerns known, as well as through officials and political channels.

Certainly, my understanding of the adequacy challenge is that it is not the only way of exchanging data. We do not want to lose it—we have been clear about that—but there are other ways of achieving the data exchange that we need outside of those arrangements.

Baroness Ludford: Lord Jackson picked up on the point that I wanted to drill down on. I note that Mr Ayling has a couple of times now—that was the third time, I think—envisaged that data adequacy and public safety could be not only juxtaposed but opposed. I must confess that I struggle to see that. Mr Jones slightly added to that by saying that data adequacy is not the only way to get the data, but what you have been saying all the way through is that it would even clunkier than it has been since Brexit. If it is more difficult to get hold of data, which is essential to fighting crime and keeping people safe, surely data adequacy and public safety go in parallel, not opposite, directions. I do not really understand how it could be anything other than a potential threat to public safety to lose data adequacy under the law enforcement directive.

Peter Ayling: As I have raised it—although, in fairness, the third time I did so was only in response to the question—I will start. I think you are right: they are complementary in the overwhelming majority of circumstances. I suppose it is not impossible that tensions would arise where all efforts were to maintain data adequacy that might require you not to use, or not to be able to retain, data in a way that you thought was optimal in the interests of public safety.

Baroness Ludford: But you might not get it in the first place if you did not have data adequacy.

Peter Ayling: That is a very important point, hence I am pleased that such issues are not currently exercising me. If there were a tension, it would be important to have mechanisms to raise and respond to that. It might well be that a stronger case could be made in the interests of data adequacy than for the one particular element that, taken in isolation, pertained to public safety, but you would have to have confidence that those conversations could be had, that legal advice could be heard and that remedy could be sought. That is where I have confidence, because that is part of the system response to tensions that might arise, either now or at any time in the future.

The Chair: Thank you for that very useful exchange.

Lord Stirrup: I just want to go back to the issue of data adequacy versus workarounds, if we were to lose it. So far this afternoon, we have talked in terms of broad, general principles, but I want to take a specific instance and see how it applies to that. One of the key issues focusing political minds across Europe is illegal migration. One of the effective ways of dealing with that is a pan-European police effort to target the people smugglers, but that requires a lot of cross-border co-operation; of course, that involves information flows as much as anything else. I will not ask you to comment on what is actually being done—nor would you answer if I asked you—but to what extent would such a pan-European effort be hampered if we had to use workarounds and lost data adequacy?

Robert Jones: We are able to exchange, and would still be able to exchange, data through Europol and Interpol channels, notices, diffusions and intelligence logs. Those are source-protected and sensitive intelligence; the recipient can then make their own mind up about their assessment and action. This is what feeds a lot of the operational response in relation to a lot of serious organised crime. That is what we would seek to do.

I would separate the issues around migration, migration flows, the flow across Europe from source countries and immigration policy from the exchange of data on organised crime that feeds investigations. For that, I am confident that there are channels where we could carry on exchanging information.

Peter Ayling: I have nothing to add to that.

Q71 **The Chair:** In our last minute or two before we let you go, I have one last thought. I want to go back to the Prüm discussion—how important that is, how useful it has been and how we have, in effect, maintained current levels of access, which is positive. We are hearing about proposals for a Prüm II from the EU—indeed, a regulation has now been agreed. We need to consider that. It includes facial recognition data in the database, I think. Have you taken a view on whether you think access to that would be helpful from the point of view of law enforcement and policing in the UK?

Robert Jones: We are looking at all the additional Prüm proposals. When it crystallises into a solution, we can make those considerations and make a decision. One of the benefits of that data is that we do not have to be part of the EU to be a partner. We know that it works and that that exchange works, so we would be very keen to exploit every opportunity there in future.

The Chair: Thank you very much indeed. We have finished nicely. We have not been disrupted by votes, which is always a positive. I thank you both for a very interesting, frank discussion. It has been very helpful to the committee—many thanks.