Select Committee on the European Union

Home Affairs Sub-Committee

Corrected oral evidence: The EU Data Protection Package

Wednesday 1 March 2017

10.45 am

Watch the meeting

Members present: Baroness Prashar (The Chairman); Lord Condon; Lord Cormack; Baroness Janke; Lord Jay of Ewelme; Baroness Massey of Darwen; Lord O'Neill of Clackmannan; Baroness Pinnock; Lord Soley.

Evidence Session No. 2 Heard in Public Questions 9 - 21

Witnesses

I: Stewart Room, Partner, Global Cyber Security and Data Protection Legal Services leader, and UK Data Protection leader, PricewaterhouseCoopers LLP; Professor Valsamis Mitsilegas, Professor of European Criminal Law, Queen Mary University of London; Rosemary Jay, Senior Consultant Attorney, Hunton & Williams.

Examination of witnesses

Stewart Room, Professor Valsamis Mitsilegas and Rosemary Jay.

Q9 **The Chairman:** Good morning and thank you for your time. I will make clear that this is a public session and it is being webcast. You will be sent a transcript of the proceedings and, if there is anything you wish to correct, please feel free to do so. If after the proceedings you want to send us any supplementary evidence, again feel free to do so. Can I start by asking you to introduce yourselves and tell us a bit about what you do?

***Professor Mitsilegas*:** I am Valsamis Mitsilegas. I am a professor of European criminal law and head of the department of law at Queen Mary University of London. I have been working for a number of years in the field of EU justice and home affairs law. In this session, I am mostly coming from the perspective of public security, data protection and privacy, and the relationship between state surveillance and human rights. It is great to be back.

***Rosemary Jay*:** My name is Rosemary Jay. I am a lawyer with a firm called Hunton & Williams. I have been working on data protection since 1987, when I first joined what was then the Office of the Data Protection Registrar. I subsequently headed a private practice. I write academic textbooks on data protection and still advise clients in the area.

***Stewart Room*:** Hello, my name is Stewart Room. I am a partner at PricewaterhouseCoopers LLP. I am the global head of cybersecurity and data protection legal services, and the co-lead of our global data protection practice. I generally act for businesses.

Q10 **The Chairman:** Can I begin by asking something about the whole of the EU data protection package? We are looking at all four elements: the general data protection regulation, the law enforcement directive, the EU-US privacy shield and the EU-US umbrella agreement. It would help the Committee very much if you could describe in broad terms the implications for the UK in terms of the impact on UK businesses and other data controllers and on people whose information is being shared: that is, data subjects.

***Stewart Room*:** Currently, the impact of the GDPR will be felt through the automatic adoption of the regulation, through our normal procedures. After we leave the EU, the critical consideration will be the extent to which the UK is perceived to be adequate, from the EU's perspective, for data protection.

On the question of the business impact of the regulation, the regulation essentially provides a code for good business practices and for the good handling of personal data. If we were to strip out the legal components of it and the enforcement mechanisms, we would find a framework within the GDPR that most businesses would agree are necessary for good data

handling. Citizens—members of the public, employees, customers and consumers—will be given more rights over their personal data, such as greater rights to transparency and greater rights to intervene in the operation of business if they have concerns and worries. There is a compulsory breach disclosure law, which will help citizens to understand if there has been a serious incident concerning confidentiality and security, which is both a transparency mechanism and a mechanism to help them mitigate any harm. In that sense, the GDPR provides a good framework for business and additional rights for consumers.

***Rosemary Jay*:** Overall, in terms of the pattern of application, the police and criminal justice directive will focus on competent authorities. There is quite a strong divide between the two, so we are not looking at an overlap of those two jurisdictions. The privacy shield is focused on commercial uses and those who are in the private sector. There is quite a strong divide, which we should flag, between the impacts of the two pieces of legislation. There are significant overlaps in content between them, but they are not on all fours and you are looking at two patterns, not just one.

***Professor Mitsilegas*:** I will say a few things about the context of these measures under European Union law. The data protection regulation and the data protection directive aim to provide standards for internal EU law purposes. They are there to amend pre-existing EU laws. The very important 1995 EU data protection directive has been replaced with the regulation, and the current directive replaces the 2008 framework decision. As Rosemary said, the regulation covers the private sector and the directive covers the police, although sometimes the distinction is not that clear, as we will probably see today.

The other two instruments are part of the EU's external action and have been adopted in a reactive way, in order to address concerns over the onward transfer of EU data to third countries, including the United States. There have been responses, primarily triggered by political events such as the Snowden revelations. There are very big concerns about the fate of personal data once they reach the United States. There have also been rulings by the Court of Justice, particularly in the case of Schrems, where the Court of Justice annulled the Commission's adequacy decision, which is its finding that US law provided adequate data protection to commercial transfers. The privacy shield is a response to the court's ruling in Schrems. It covers private sector data. The umbrella agreement is a response to the post-Snowden controversy. It covers law enforcement co-operation. This is the external side of the internal EU measures, which is probably why it is called a package.

The Chairman: That leads me to the next question. Can you identify the key differences between the EU regulatory framework governing data exchanges for trade and commercial reasons and that governing data exchanges for law enforcement purposes?

***Professor Mitsilegas*:** I will answer in one sentence, and maybe colleagues can add to it. The law enforcement instruments contain more

nuance. In practice, the rights and principles in the regulation and the directive are the same—for example, the principle of purpose limitation or the right of access to personal data. However, the law enforcement measures contain more exceptions, to take into account the needs of law enforcement. They give national authorities greater discretion to limit the rights of individuals in certain circumstances.

***Rosemary Jay*:** Although the structure and key requirements are very similar, there is a big difference, in that the regulation of the law enforcement sector is national. This will obviously be affected by how things pan out in the future, but under the regulation as a European measure there is what is called the one-stop shop. There is a European Data Protection Board, a pan-European authority with significant authority to take the lead on enforcement-type decisions. The fines are set at a high level. The police and criminal justice directive is purely national. The board has an advisory role to promote consistency, but there is a big difference in practical application. For criminal justice, there are some specific rules about types of data, such as that of witnesses, and retention. Although there are great similarities in structure, there are still differences. I hope that helps.

***Professor Mitsilegas*:** Can I make one more point on the nature of the legislation? We talk about the regulation and the directive. The regulation, under EU law, is an instrument that is directly applicable from the day of its adoption, as you will probably know if you have examined this already. It is law, and one size fits all across the EU member states. The directive gives member states breathing space: they have to implement it, taking into account their national particularities. In the field of criminal justice, this is very important.

Q11 **Lord Jay of Ewelme:** As you can imagine, we have been looking at the implications for Brexit of a number of the issues coming before us. I want to turn to the Brexit implications, or some of them, of the EU data protection package. We heard from the Information Commissioner's Office recently that when we leave the EU, assuming that we do, we will be treated as a third country on data protection issues, so we will require an adequacy decision from the European Commission once we have left. My first question is this: assuming that we will be treated as a third country on data protection once we are no longer a member of the EU, what would be the default position as a matter of law for data flows between the UK and the EU if we have not secured an adequacy decision or equivalent arrangement at the point when we leave the EU? It would be very helpful to me if one of you, perhaps Mr Room, could explain what an adequacy decision is and how difficult it would be to get.

***Stewart Room*:** I am very happy to do that. An adequacy decision is a process that is led by the European Commission whereby it examines not just the legislative framework of the third country but other matters that are critical to data protection, such as custom and practice. For instance, professional codes of practice would be significant in the legal sphere or the accountancy sphere. In medicine, we have very sophisticated codes

of practice for patient confidentiality. The adequacy decision has to look at the totality of the legal system in the third country.

On the question of where we will be afterwards if we Brexit without an adequacy decision, at the moment most countries in the world do not have an adequacy decision—that is the point—yet they are able to receive personal data from Europe. A range of mechanisms can be deployed or utilised to maintain the flow of data from Europe to third countries that do not have an adequacy decision. For example, Europe has developed a set of contractual clauses that can be put in place between an entity in Europe and an entity in a third country that would permit data flow, despite the absence of an adequacy decision. The default position is that the UK would have to rely upon these other mechanisms to maintain the movement of data from Europe into our country.

On the question of the process and the time that these decisions can take, as I said, there are not many of them.

Lord Cormack: How many are there?

***Stewart Room*:** There are approximately nine. Rosemary might know the exact number.

***Rosemary Jay*:** Nine sounds about right. I could check.

***Stewart Room*:** Places such as Andorra, Argentina and Israel benefit from adequacy decisions, but the United States does not, except in the context of the privacy shield, and Canada does in part.

Lord Jay of Ewelme: Is that because they have decided not to apply for it or it is not relevant to them? Would it be relevant to us?

***Stewart Room*:** There is a combination of factors. Countries wish to gain a badge of adequacy due to the perception that it would be helpful for global trade.

Lord Cormack: For Andorra, it must be.

***Stewart Room*:** Indeed. We have a range of drivers, from countries seeking an adequacy decision because they perceive it to be a good thing for them to the European Commission working from its own incentive. There can be a combination. The point about there being only nine is also an indicator of the amount of time and complexity that attaches to the development of an adequacy decision. My point is that they can take many, many years.

Lord Cormack: Of the EU27, how many have these adequacy decisions?

***Rosemary Jay*:** They do not need them. They are part of the club.

Lord Jay of Ewelme: If we did not have one, what would happen? What would the alternatives be for us if we did not have an adequacy decision? Would that prevent us having the sort of data sharing

arrangements that we now have within the European Union if we were outside it?

***Stewart Room*:** As I said, in the absence of an adequacy decision, there are other legal mechanisms. Business-to-business transactions could be maintained through the adoption of the contractual scheme that Europe has approved. In the absence of an adequacy decision, UK businesses would look at creating contractual relationships with their business partners in Europe. For a multinational group of companies that is headquartered all over Europe, around the world and in the UK, there is a mechanism called BCR—binding corporate rules. That allows multinationals to share data across the group globally. We, or our companies, would need to look at such mechanisms.

The problem with the absence of an adequacy decision is that it can provide a platform for other people to criticise the UK and to challenge the UK's adequacy. If we are not adequate and someone wants to cause trouble or has an issue that they would like to ventilate, they could say, "This country is not adequate", and trigger the various legal processes that were triggered in the safe harbour case the professor mentioned in his first remarks.

***Professor Mitsilegas*:** I have two points to make on adequacy. First, you have to bear in mind, as we saw in the case of Schrems, that the European Court of Justice is raising the bar on adequacy. There is a big question about what we mean by adequacy when we ask, "Is the data protection framework with a third country adequate, and does it provide adequate data protection?" The Court of Justice in Schrems, which involved the US so we are not talking about some third country with no system, said that the two systems need to be essentially equivalent. The Court said, as Stewart said, that it is not enough to tick-box the legislation. You have to examine how this works in practice and ensure that data protection is provided in an effective manner. The benchmark is high.

The Commission is also obliged by the court to check regularly. In the safe harbour case, the problem was that the Commission made an adequacy decision many, many years ago, and the court said, "How do you know what is going on now? You need to check at regular intervals". Third countries that want to have an adequacy decision in their favour need to prepare for an increased level of scrutiny of their own data protection framework.

The other element is in the field of law enforcement, where things are not so easy. In private law, companies have to survive and have to exchange data, hence all these mechanisms. In the field of law enforcement, things become more complicated, because even if the United Kingdom wanted to proceed into bilateral agreements with EU member states, when EU member states act externally they are bound by EU law. They cannot co-operate with third countries if these countries are not perceived to provide an equivalent level of protection. There, I think, adequacy would be more important for the UK and for public security.

***Rosemary Jay*:** On a very basic point, the fundamental problem is the flow of data from Europe to the UK. Depending on what our law is when we get to that stage, there is no absolute reason why the UK should put up a barrier to the disclosure and transfer of data to other jurisdictions. That is not an automatic thing, although if we want an adequacy finding we have to put up some barriers in relation to third countries. The critical issue is the flow of data across to the UK.

Lord Jay of Ewelme: Presumably this is a dynamic process. If you have an adequacy decision or some alternative to an adequacy decision now, you are going to need something else in two, four or six years' time because technology develops. Is there a mechanism for that?

***Rosemary Jay*:** As I understand it, where countries have adequacy decisions under the current law and there have been findings by the European Commission, those findings will remain valid after the regulation comes into effect. In reality, the countries that have adequacy findings now are preparing to reapply, to refresh their adequacy, because they are looking to bring their laws up to speed with the regulation and the directive. There is already a queue of people who are applying to the Commission. The Commission has a policy paper on how it will look at adequacy decisions going forward and which countries it will look at over the next 12 months. Clearly, it is very resource intensive, so it has to think about its resources.

Lord Soley: Can you clarify something, Mr Room? You said that if a company or organisation was not satisfied, it could issue a challenge and trigger the legal processes. Can you tell me whether, in cases where that has happened or, indeed, where it might happen, is it done essentially for competitive advantage? What is the reason for doing it?

***Stewart Room*:** It is a very good question. We have one very clear example of this and, as the professor mentioned before, it related to the aftermath of the Edward Snowden disclosures. We have heard the name Schrems being mentioned; he is a well-known privacy advocate. In that case, the legal mechanisms were triggered. They were first triggered in Ireland, by way of complaints about the transfer of data by Facebook to California. That moved to the Irish High Court after the Irish regulator failed to intervene. The Irish High Court referred the matter to the Court of Justice and the litigation proceeded to judgment. That was in October 2015, off the top of my head.

As a result of that, the EU-US safe harbour agreement that had essentially governed a lot of transatlantic data flow for 15 years or so was declared invalid. As a result, the privacy shield, which is one of your topics, was implemented. We now have two challenges to the privacy shield along the same lines, involving one of the litigants in the safe harbour case. Those cases seemed to be motivated by two aspects. One was the quality of human rights protections in the United States; it was a pure privacy component. There was also a sense of a political dynamic within it. We have not detected litigation of this nature being pursued for

economic gain or to cause economic disadvantage. That is how I would put it.

Lord Soley: Could you see that emerging? Could you see a company saying, "If we stop this company from coming in, we will have an advantage"?

***Stewart Room*:** Yes, there is always the theoretical risk that another business might do this for commercial advantages, but that would be a dangerous place for businesses to go because they would draw attention to themselves. The risk is more of the one I just described with the Schrems case, which is privacy advocacy or a political fight being run through the auspices of this legal mechanism. If it was to happen, those are the most likely drivers for this litigation.

The Chairman: In a nutshell, can you explain the benefit of an adequacy decision over relying on other fall-back mechanisms? Is it just to prevent future legal challenge?

***Stewart Room*:** I have given a lot of the answers here. I will put it simply from a commercial perspective and let my colleagues give you more from a legal perspective. Multinational businesses want to build to a common standard. They want certainty. They want to build their technology systems, digital environments and cyber positions to a single common standard. An adequacy decision gives certainty to businesses and to the economy that the United Kingdom's law is accepted as being of the right nature and having the right properties. When the safe harbour case came through, despite there being other legal mechanisms that businesses could deploy, they were lost in the argument. People reacted with a sense of panic to a potential data transfer catastrophe. Businesses do not necessarily look at the nuanced legal position that we have mentioned. From a commercial perspective, that is the critical dynamic.

The Chairman: That is very helpful.

***Rosemary Jay*:** Safe harbour, or the privacy shield as it is now, is an atypical adequacy finding. It is very different from all the rest of the adequacy findings. The rest of the adequacy findings, even the Canadian one, which does not cover all data flows, are formal legal decisions and legislative acts of the Commission under which the Commission, as a matter of European law, finds that the legal system in the state as a whole is of equivalence and that therefore there can be no barriers to the flow of data to that state. A business that sought to say, "We are not sending our data because it is inadequate", would be acting unlawfully. You would be able to challenge that in the court. An adequacy finding for a state is the strongest guarantee of the free flow of data in terms of the commercial environment.

***Professor Mitsilegas*:** In terms of security, the fall-back is even less clear, so adequacy will give certainty, including to the law enforcement authorities of the remaining EU member states.

The Chairman: Thank you for that. That is a good clarification.

Q12 **Lord O'Neill of Clackmannan:** In the context of Brexit, would you expect it to be straightforward to negotiate an agreement with the EU27? At the moment, one would imagine that the UK's standards are on all fours with the 27. Would that enable us to arrive at a point-of-departure arrangement, which would allow us to keep abreast of changes within the EU in the future?

***Rosemary Jay*:** I just said in my answer that an adequacy decision is a formal, legislative decision of the EU. The Commission actually has to make that decision. It has to go through a legislative process. It is not simply within its gift to do it in some informal way. At the moment, it has to go to the Article 31 Committee and then the Article 29 Committee; then the Commission has to make its decision. I can see no way that that could be foreshortened. An adequacy decision is a decision made in relation to a third country. Technically, I do not think we can get to adequacy in that sense before we become a third country. It just seems logically that we cannot do that. There is a legislative barrier. I cannot comment on whether there is some procedural mechanism such that the process is expedited the day we walk out. In my view, it would be optimistic to hope that, but I am happy to take other people's views.

***Stewart Room*:** The issue about the ability to conduct a negotiation has to be seen in the context of all the issues and which are perceived to be priorities. I sense a slight difference between the topic of data protection and some of the other topics that would need to be addressed, such as trade barriers. The essential point about data protection is that all of Europe, regardless of the nature of the EU, believes in this subject matter. The data protection regime flows from the Council of Europe; of course, you fully understand the history of that after the Second World War. There is an interest for all EU member states to maintain strong data protection. The 27 would want to see strong data protection for their citizens who remain in this country afterwards. If you are a French-headquartered multinational, for instance, you would want to ensure that the French Government achieved the same form of data protection in this country.

For all these aspects, there is a very clear global interest, not just a European and UK interest. If we were to take just one dimension of this, security and cybersecurity, which is one of the principles of data protection, there is not a single member state arguing a different narrative about cybersecurity. Everyone wants to achieve the same outcomes. There are very strong incentives for people to treat this in a different way potentially from other issues.

Lord O'Neill of Clackmannan: Is this one of the areas that the UK has played a significant role in? In policing, Britain had if not established a number of the European co-operative arrangements then played a leading role in them. Would our departure from this process create something of a vacuum? Could that be taken advantage of? I do not mean that in a brutal way, but could it be used as a negotiating counter if

we were trying to get some kind of interim agreement?

***Professor Mitsilegas*:** This cuts both ways. You are right that in the field of criminal justice the UK has been a real contributor to the development of European integration in the case of both Europol and the European arrest warrant. In this field, the security aspect of things, the UK has been instrumental in convincing other EU member states to increase access to personal data by law enforcement authorities through the data retention directive, the new directive on passenger name record data and so on. However, we have increasingly heard the Court of Justice saying that some of these arrangements are not constitutional under EU law. You may have followed the judgment given before Christmas in the case of Watson and Tele2, where the Court of Justice essentially said that domestic UK arrangements on data retention were contrary to EU law. There is tension there.

On the substance of your question about where we go now, adequacy will be seen in terms of domestic UK law. While in the case of private law and the data protection regulation it is very likely that we will see a level playing field, in the field of security there may be challenges for the UK if EU member states and the Commission perceive that UK data protection law is of a lower standard than EU law as interpreted by the Court of Justice. That will not be as easy in this context.

Lord O'Neill of Clackmannan: You mentioned the European Court of Justice. For a number of those who advocated leaving, the ECJ is something of an anathema. Are you saying that, in order to have a post-departure relationship, we could not ignore or it would be very difficult to ignore the European Court of Justice, in much the same way as the United States, which always argues for US exceptionalism? We would have to find a mechanism or not, in the light of the US experience. Would that be relevant?

***Professor Mitsilegas*:** You are exactly right. In the field of criminal justice, EU law and the EU acquis are as interpreted by the Court of Justice. In the field of data protection, we should not forget that the Court of Justice interprets the instruments, the regulation and the directive, in conformity with the EU Charter of Fundamental Rights, which is part of EU law after the entry into force of the Lisbon treaty. This means that compatibility, equivalence or adequacy under the data protection directive or regulation will be assessed by the Commission in light of the interpretation of these instruments by the Court of Justice. However you define the legal relationship and the impact of the court, while you can say it has an advisory role, in reality, when the assessment is made, the Court of Justice's case law must be taken into account.

Q13 **Lord Cormack:** This is very much a layman's question and I accept the point you made about not needing adequacy at the moment within the European Union. If you were looking at us alongside the other European Union states at the moment, would you rate us as being very adequate or inadequate? Is it possible, when we leave, to be judged adequate in cybersecurity, say, but not in other areas? Can you just clarify that?

***Stewart Room*:** It is a very good point, because it follows from Lord O'Neill's point about the UK as an influencer and where we stand. From my personal perspective, currently, the UK is not just adequate on data protection but in many areas far exceeds many other EU member states. If we look at the supervision and enforcement mechanisms and the UK Information Commissioner's Office—Rosemary will be able to pick this up because she used to work there—the output, guidance and assistance that the UK provides to the economy and to the European and global economy, in the development of codes of practice for businesses, by far and away exceeds most other member states. In that sense, we have an enforcement and supervisory regime that is better than most. If you were to look at the number of cases that are reviewed per annum by the UK Information Commissioner, the workload is greater. We have that component as well.

Another point concerns the fora and networks that exist outside these legislative and political structures. For instance, we have an enforcement network called GPEN—the Global Privacy Enforcement Network—which consists of many global regulators, not just the EU but the Federal Trade Commission in the US. The UK is instrumental at the heart of that. We have another enforcement network called the Common Thread, which consists of all the Commonwealth member states, which the UK has led the development of. These are systems and fora that should give us confidence that the UK will have influence behind the scenes and potentially at the sharp end of data protection. That is how I would put it in layman's terms, in terms of where the UK is.

***Rosemary Jay*:** It is a long time since I worked at the Information Commissioner's Office, but I would probably say that I completely agree, on a hard analysis, that that is the case. However I do not necessarily think that that is how we are seen in Europe. There is a gap between that and the popular cultural view that the UK is soft on regulation, including data protection. I completely agree that the UK is one of the most effective regulators. Unfortunately there are popular myths, which are very hard to dislodge, which do not reflect that reality.

Lord Cormack: There are misperceptions.

***Rosemary Jay*:** Yes.

Baroness Janke: In the case that you mentioned, are we talking about deficiencies in the protection of individuals, human rights and that area, rather than the letter of the law that we have as regards the Data Protection Act?

***Rosemary Jay*:** I read some of the transcripts from the Schrems court hearing. There is occasionally a flavour to the comments that seems to suggest that Ireland and the UK do not take data protection as seriously somehow as other jurisdiction in the EU. It is difficult to put one's finger on, but I would just flag it as a counterpoint. I agree completely that we have a very effective regulatory body. I am not completely certain that that is the popular view throughout the EU.

Baroness Janke: The Snowden revelations certainly gave the impression of a very oppressive supervisory regime in this country, even more so than the United States.

***Rosemary Jay*:** I do not know.

***Professor Mitsilegas*:** I partly agree with you. There is a differentiated picture. In terms of the regulation of private companies, the standards are quite close together and there are various co-operative mechanisms. In the field of security, there are concerns about the United Kingdom. Let us not forget that the United Kingdom was found to be in breach of EU law in the case of Watson just before Christmas. On the topic of mass surveillance on the basis of bulk collection of personal data and the transfer of this data to the law enforcement authorities, this is a red line for EU law now. It is against EU law and, as long as you have domestic law that allows mass surveillance, you will have problems with EU law. This is not exactly the same as saying that the UK does not have adequate data protection supervision mechanisms in its own system. It does, but, when you have political choices that say that more and more personal data should be collected indiscriminately, this causes problems for EU law.

The Chairman: Those are very helpful answers. Can I summarise, in order to understand for my own purposes? Are you saying that there should be a mutual interest in getting the adequacy decision for the UK but sequencing might be a problem?

***Stewart Room*:** Sequencing will need to be figured out during the processes that will now follow, but the mutual interest is absolutely clear, on any measure or test.

Q14 **Baroness Massey of Darwen:** Post Brexit, how much room for manoeuvre on data protection policy do the UK Government have in practice, if they want to maintain unhindered flows of data with both the EU and the US?

***Stewart Room*:** One way of looking at this would be to consider the GDPR, which is a regulation and has direct applicability. Most of the things that businesses and other organisations will have to do operationally, as it were in real life, are not yet described in the GDPR. The mechanics of doing things and the road map or the A to Z are not there. They will have to come from somewhere. The primary source will be via regulatory guidance, for instance. As I mentioned before, we can look at particular sectors, such as the health sector with the Caldicott principles for patient confidentiality. My point is that there is very significant space inside the GDPR framework for the United Kingdom to develop its positions for day-to-day operationalisation of this subject matter, provided of course that the principles of data protection and the rights are obeyed.

***Rosemary Jay*:** I would agree with that. There is scope. The UK, for example, has a strong freedom of information regime. It has a deep

commitment to freedom of expression. It has wide exemptions for freedom of expression in the current law and, potentially, the ability to replicate those in its future law. There is scope within the GDPR framework for us to continue focusing on those things—for example, medical research—where we have huge resources and capacity, and to continue leading the way in areas such as fraud assessment and prevention. When one talks about room for manoeuvre, I agree that we are not looking at avoiding the framework and strictures of the GDPR or lessening digital security, because that digital trust is going to be very important going forward. The GDPR does not stultify many of the things that the UK can lead on and has strong practices in.

Baroness Massey of Darwen: What changes to the UK data protection regulatory landscape would you like to see after Brexit? What opportunities will be available?

***Rosemary Jay*:** Post Brexit, the starting point will be that we want to see the GDPR in operation and to an adequate level. That is critical. It is the most commercially important thing for business, throughout the sectors. Within that, there are some elements of leeway. For example, there are quite wide exemptions for research. The UK has some leeway to look at those. Our research in oncology is world leading and we can make sure that we maintain the support that we have for those kinds of industries. It is more about looking at that framework and looking for the positives as to what we can do in the right way going forward, rather than trying to avoid the regulation. As both my colleagues have said, it is offering protection for individuals and frameworks for business in a digital world.

***Stewart Room*:** If we focus on the importance of certainty for businesses, particularly multinationals, having a GDPR Act where the legislation is transposed verbatim will be a significant advantage. Another component must be the ability of the regulator's office to be relevant and penetrative and to lead. If adequacy comes into play, as I said, it is not just the legislation, but the reality of how it works. We need to ensure that our regulator is sufficiently resourced in terms of skill and capability, so that no one can levy the charge that the data protection regime is not working in operations. If that charge was to be levied and we had a political problem about adequacy or not, that is the place where I would start if I was advising the other side.

Q15 **Lord Condon:** I wonder if I can explore something that you have already raised to some extent, Professor. It has been suggested to us that, in the field of police, security and law enforcement, the UK has been a very influential voice in Europe in the debates about data protection. We have perhaps been a moderating voice in setting the balance between the needs of privacy and the needs of the state. Post Brexit, that moderating voice will clearly be absent, officially, and there will be a movement more towards privacy and the needs of individual citizens, in a way that might be challenging for our Government and law enforcement agencies. Is it a valid assertion that, when we are not at the table, Europe will perhaps move more stridently towards privacy of the individual, or is that a fear?

I am not asking you to make a value judgment about where the balance should be, but does our voice matter and what will happen when we are not there?

***Professor Mitsilegas*:** It is hard to predict the future, and the actions of Governments depend to a great extent on events. If we look at where we are now, we have indeed seen the UK being very influential in convincing other EU member states to expand surveillance. We mentioned the data retention directive, which was a UK initiative, and the more recent directive on the transfer of passenger records when they fly into the EU. These are both instruments for which the UK advocated strongly. However, the logic of some of these instruments has also been challenged before the Court of Justice. The data retention directive has been annulled, in the case of Digital Rights Ireland. EU law is, in a sense, rebalancing itself and the different EU institutions are repositioning themselves.

Bearing this in mind, I am not sure whether we can definitely say that the future will be pro-privacy, because I am sure other Governments in the EU will push for further law enforcement access if they perceive the population as being under threat. From where I am coming from, and as a more general point in the field of criminal law, on which I know the Committee has completed an inquiry, the UK absence from the negotiating table will be a loss for the EU and the other member states, because the UK has always been very constructive as a negotiator and in terms of the substance of the instruments.

***Rosemary Jay*:** I would agree with that.

Lord Condon: Linked to that, when we are out of the EU, are there other mechanisms through which we can seek to exert an influence on the areas that we have just explored? Mr Room, you explained how in many ways we are a world leader on some of these issues. Will that reputation be enough for us still to exert an influence over the agenda in Europe?

***Stewart Room*:** In this area, I am sure, yes. People who have to deal with these subject matters in an operational sense know that they have to solve problems while the political situation is being resolved. People come together, in the law enforcement field, to solve problems. I do not perceive any sense at all that the UK's skill and leadership are not valued on these subjects.

Q16 **Baroness Janke:** Pending the Government's impact assessment for the prospective legislative change arising from the regulations and the directive, can you give your assessment of the resource implications for business of complying with the GDPR, the law enforcement directive and the EU privacy regulation?

***Stewart Room*:** Yes. If you look today at businesses that are getting ready for the GDPR, lots and lots of GDPR programmes are now in flight, as you would imagine. They have significant capital and resource costs associated with them. However, part of the issue to understand is the extent to which organisations will be spending this money to improve

themselves to a new standard, or to catch up on things that they should have been doing under the Data Protection Act 1998 and that they have failed to do.

A good example would be in terms of data retention. What we have discovered as a problem in the economy is that, with the ability for electronic or digital data to proliferate, it has proliferated beyond the expectations of the Data Protection Act 1998. Many organisations, in a technical sense, are retaining electronic data that may not be lawful under the UK's current regime. The GDPR causes them to focus on the subject afresh and they discover a data lake that needs to be drained, so that capital cost is incurred. Arguably, they are incurring that capital cost because they have not worked on the Data Protection Act, not because the GDPR is requiring anything new.

The way I would put it is that the principles and the rights of the GDPR and all the build requirements we have—ideas such as privacy by design and privacy impact assessments—are needed to run technology in any event. They are just being codified because a lot of organisations have misunderstood this, which is part of the explanation for the cybersecurity problem that we have in the economy right now.

***Rosemary Jay*:** I will pick up on what Stewart has said, and perhaps you can say something about the policing, because my sense is that our policing standards are very good in relation to Europe overall and we do not have a huge gap in terms of the police and criminal justice directive. I will let you comment on that, perhaps. There are some things in the regulation that are not catch-up and are going to be new. The security breach notification will be a new requirement. That will have a resource implication, but, given the importance of cybersecurity and the way we should be focusing on security breach, one might say that it is a resource that businesses should be looking at.

More of regret are the internal recordkeeping requirements and some of the details of the notice requirements, which are heavier than one might have liked. Having said that, we have become more adept in business at looking at ways of giving notices and producing layered notices. We also see some appetite for people to have more of a sense of what is happening to their data and to understand more. Walking into that area is not necessarily a bad thing for citizens and business in the long term. In terms of data portability, given the details of internal recordkeeping notices and security breaches, additional resources will be needed. We have only had the draft of the new ePrivacy Regulation since January, so it is hard to evaluate the impact of that. The big issue there is the extension of the scope to cover all added-value services, which is difficult to quantify. Are you going to say something about policing?

***Professor Mitsilegas*:** I agree with you. The police should have been following what is in the directive anyway. I do not see any huge burden coming forward.

***Stewart Room*:** We need to look at the positions of small to medium enterprises. That is part of the reason why I hold the view that we need a strong regulator. Large multinationals can procure professional services support that can help them to understand how things should be done, but that is not necessarily the same for every organisation in the economy. There is a space where a strong regulator really works. If the regulator can create guidance, to-do kits and toolkits, it will reduce the resource load on small businesses. That is very important to look at.

Baroness Janke: The real movement in digital work is about sharing information more and more across services, for example. Some of the current legislation is apparently going in a rather different direction. If you are saying that people are not complying with the Data Protection Act, it is a worry from the point of view of satisfying standards elsewhere.

***Stewart Room*:** Yes, of course. This is why I hold the view that, if you look at the GDPR not as a legislative thing, but as a user guide for the critical asset of technology data, this is what we would want to see in the economy, because the problems of failure around this are just too important to ignore.

Lord Cormack: This follows on from what you were saying about needing a strong regulator. From all the evidence that we have received on a variety of subjects, it has become increasingly apparent to me that we will have to have perhaps the most broadly based and sophisticated embassy that we have ever had in Europe when we come out. Do you think it is crucial that we have people at a very senior level on your subject as part of representation in Europe?

***Stewart Room*:** We need to be in this conversation, however that structure is built and whatever it looks like. We would want to provide as much expertise to the design of this framework as possible, because if you build a mechanism that is not thought through and that leads to failure, such as a technology system falling down to hackers, that is in no one's interest. We want to bring as much as possible of the economy, not just Europe but the global economy, to a standard that we perceive protects our interest. However that is represented, data protection must be part of it.

Q17 **Lord Soley:** This is to do with the EU-US privacy shield. To some extent, you have been circling around issues like this. Post Brexit, when we are no longer part of that privacy shield, can you see us having a separate agreement with the United States? What form would that agreement take?

***Professor Mitsilegas*:** There is nothing stopping the UK having a bilateral agreement with the United States on the transfer of data. The challenge there, in terms of standards—and my colleagues can perhaps expand on this—would be whether the standards need to be equivalent with EU standards if you want to ensure maximum data transfer across the board, so you know that the UK-US agreement or any arrangements that exist would allow multinational companies to use this data in the

context of EU operations. Legally, if the UK is a third country, it would certainly go ahead and try to conclude an agreement, an arrangement or a code of practice with the United States.

Lord Soley: If we had a situation where we already had adequacy with the EU, we could create an agreement with the United States based on that adequacy as long as the US was prepared to negotiate on that basis.

***Professor Mitsilegas*:** It could even be a tripartite venture along those lines.

***Rosemary Jay*:** Switzerland has equivalence. It sits outside the EU and has a separate mirror agreement with the US. Switzerland has an adequacy finding and a mirror agreement, so the flow of data from Europe through to Switzerland, through to the US and round back again is unimpeded.

Lord Soley: It has done what I was hinting at in my question. The adequacy bit is what needs to be reflected in the agreement with the United States. Is that right?

***Rosemary Jay*:** Perhaps I have not explained it. Switzerland has an adequacy finding, so it is regarded as equivalent and adequate, and then has a mirror of the privacy shield agreement with the US.

***Stewart Room*:** That is exactly right. In the way it has worked, Europe has taken a lead to build with the United States the overarching framework, and then it has been copied for Switzerland. There is no reason why that could not work.

Lord Soley: You could do that.

***Stewart Room*:** Yes, precisely.

Lord Soley: Could you do it fairly quickly?

***Stewart Room*:** If we are at the front of the queue on things, maybe so. Another point to note about the privacy shield, as I was saying at the beginning, is that it is not the only mechanism. We need to be conscious that there are alternatives. Last night, I checked out the number of companies that have adopted privacy shield, and it is only 1,700 multinationals. It is not the default choice for US-headquartered multinationals to move data from Europe to the States. If they are using anything else, they are using the model contractual clauses that we talked about at the beginning. Privacy shield is still a fringe mechanism in the corporate environment.

Lord Soley: That is an interesting one and leads me to my next question. How important is the privacy shield to UK companies?

***Stewart Room*:** It is not the default choice for UK companies sending data to the States. The default choice at the moment is model clauses

and bespoke mechanisms that are built around those European platforms.

***Rosemary Jay*:** I would just caveat that the big cloud providers are generally privacy-shielded. I would not like to put a figure on the extent of the data flows, but an awful lot of data will flow through the big and very big cloud providers. One would have to do quite a nuanced look at the sheer numbers and the actual size of the data flows. As I understand it companies such as Hewlett-Packard, Google and Microsoft are all privacy-shielded. Those are big data flows.

Lord Soley: Therefore, it is very important to UK companies.

***Rosemary Jay*:** It is certainly very important to US companies, because they can take the data. The corollary is that it is important to the European companies that deal with those US companies.

The Chairman: You mentioned US companies. Would they be very keen to negotiate a privacy shield agreement, and how long do you think it would take?

Lord Soley: Ask Mr Trump.

***Professor Mitsilegas*:** The US was very keen to conclude the privacy shield with the EU. As to the standards of international negotiations, the fact that we heard this soon, only the following year, after the court's ruling in Schrems testifies to the importance of this for both sides. In terms of the UK, it will depend on the commercial interests at stake and how big a priority it would be for the two parties.

The Chairman: Can you remind me how long Switzerland took to negotiate? How long did that negotiation take?

***Rosemary Jay*:** It was almost immediate because Switzerland has mirrored the privacy shield there was very litte delay.

Q18 **Lord Condon:** I would like to take your guidance on a couple of aspects of the EU-US umbrella agreement. While we are subject to the umbrella agreement before we leave, we currently have UK-US bilateral agreements: things such as the mutual legal assistance treaty and the extradition treaty. Are they in any way challenged or superseded by the umbrella agreement, or is one a subset of the broader, higher level? Is there anything to say about how those interact?

***Professor Mitsilegas*:** The main advance in the umbrella agreement is bringing EU law to the existing EU-USA mutual legal assistance agreement, because there is an agreement between the EU and the US on mutual legal assistance. The EU-USA mutual legal assistance agreement, which was an early agreement, was concluded shortly after 9/11 and contains an article, Article 9, which says that generic differences in the data protection systems of the US and the EU should not prevent the exchange of personal data. The umbrella agreement takes it a step forward, because the United States had to provide a series of further

safeguards in order for this transfer to take place. This is binding on the UK in terms of mutual legal assistance requests, because the UK-US mutual legal assistance agreement must be compliant with EU law in the field.

Lord Condon: The umbrella agreement trumps the other individual ones.

***Professor Mitsilegas*:** Yes, it does.

***Stewart Room*:** One way to look at it might be this: that the MLATs provide a legal basis for sharing, whereas the umbrella agreement and components like that are providing principles for how that data should be handled.

Lord Condon: Moving forward, when we are out of the EU, would you anticipate umbrella agreements being arranged from UK to EU and UK to US, or will we not need mechanisms that are quite that broad?

***Professor Mitsilegas*:** Again, with the EU, the big challenge for the UK is to provide an equivalent level of protection. Whether it is bilateral agreements with other EU member states or an agreement with the EU as such, the UK needs to provide a data protection level that is equivalent to EU law. In the security field, this may be a challenge depending on political choices in the UK. In terms of the US, my answer would be the same as the one that I gave on the privacy shield. Legally, there is nothing stopping the UK concluding an agreement with the USA on the transfer of data. The question is whether the standards will be high enough to enable the onward transfer of this data to the EU.

Lord Condon: Presumably it would be better to have an umbrella agreement with the EU as a whole, in the field of law enforcement, particularly if we want to have close co-operation with Europol. If there was a series of bilaterals between the UK and individual EU states, that might prove to be quite difficult in the field of Europol and EU databases. An umbrella agreement would seem to be preferable.

***Professor Mitsilegas*:** In my view, yes.

Q19 **Baroness Pinnock:** From what I have understood this morning, and this might mean that I have not have understood it at all, as the UK—I will put in Lord Jay's parenthesis, because I am ever an optimist—if we leave the EU, our position as regards data protection is going to be determined by the current arrangements that the EU has made, such as the GDPR, and the privacy shield that the US and the EU have agreed. My understanding—you will tell me if I am wrong or right—is that the ability of the UK to move away from either of those is seriously constrained. In other words, moving forward, our data protection legislation is going to be determined by the agreements that are already made.

***Rosemary Jay*:** If we wanted to carve a different place in the world, have different trading partners and not focus on trade with Europe and the US, we could do whatever we wanted. It is not absolutely inevitable we have the GDPR. We can pass whatever data protection law we want,

but in consequence it would be extremely difficult to have a finding of adequacy or to build the equivalent of a privacy shield.

Baroness Pinnock: The consequences of that are all the things that you have said this morning. Multinationals would not want that.

Ms *Rosemary Jay*: No, they would not.

Baroness Pinnock: If multinationals did not want it, their subcontractors within the UK would have to comply with their arrangements, and so on down the line. Am I right?

***Stewart Room*:** It is plainly in the interests of our economy, if we want to trade with Europe, to be on the same platform. If we do not, we run the risk of a judicial decision by the Court of Justice that prevents the flow of data into our country from Europe. That will have a serious impact.

Baroness Pinnock: We are still going to be overseen by the European Court of Justice. You do not have to comment on that.

Lord Soley: From what you have been saying, we are, if not the leader, a very serious leader in this area, in terms of protection of privacy and so on. If that is right, is the trick for the UK to have a model that meets the requirements of the European Union, the United States and maybe some of the other world bodies, and in that way to become a leader in the field and set the standard? If we took that view, set out to achieve that and instructed civil servants to talk to people like you to come up with a model, we could say that it was the gold standard.

***Stewart Room*:** This is my point. If you work from the premise that the GDPR is describing good things for data and technology, and you add in the fact that there is a massive amount of white space, someone needs to fill that white space. If the UK fills that white space via a strong regulator and industry bodies, we can have a data protection framework that in practical terms has been designed by the UK.

Q20 **Lord Cormack:** You have given us some compelling and fascinating evidence. Are your talents being sufficiently used by government at the moment? Are you being called in and asked to give advice?

***Stewart Room*:** On the data protection matters, for me personally, this is my first occasion and it has been fascinating.

***Rosemary Jay*:** There is an advisory group that I go to and have spoken to people from ministries.

Lord Cormack: Are you reasonably happy that what you are saying is being taken seriously?

***Rosemary Jay*:** Yes, to the extent that anything I say merits being taken seriously.

Lord Cormack: You are far too modest. Professor, what about you?

***Professor Mitsilegas*:** Being here is a good start.

Q21 **The Chairman:** Do you see any grounds for concern that domestic legislation could impact on the UK's ability to continue to share data with the EU post Brexit, for either commercial or law enforcement purposes?

***Professor Mitsilegas*:** In the law enforcement sphere there is a concern, because the United Kingdom is going down this route of increasing collection of and access to bulk data, which is increasingly incompatible with the EU.

***Stewart Room*:** My understanding from what I have read is that, through the Great Reform Bill, the Government's intention is to deliver the GDPR into this country. If that happens, we will at least have the right legislative framework, but one point that a number of you made is that, over time, you can diverge. That is why we need to have practical influence, with an embassy or whatever it might be, and a strong regulator, so we do not allow ourselves to diverge in such a way that people can attack the UK's adequacy.

***Rosemary Jay*:** Business will want to continue exchanging data. It is one of those things where, if there is a will, there is a way. As Stewart will know, safe harbour went down and the world went on.

The Chairman: Can I ask a follow-up question on the distinction between commercial and legal data protection? Would it be legally possible to be ruled adequate by the Commission on commercial data but not on data protection in law enforcement?

***Rosemary Jay*:** There is a provision now, under the regulation, to allow for partial adequacy findings. There are currently partial adequacy findings; there is one for Canada and the US is obviously partial. It depends on supervision and so on. That has been formalised in the regulation. We do not yet know how exactly it will work, of course, but it allows sectors and territories to be considered. It is possible that there will be more flexibility than we have seen previously.

Lord O'Neill of Clackmannan: How long does the process take to establish adequacy in one sector but not in another?

***Rosemary Jay*:** I do not know that it would be any different, because the process has generally taken two to three years from an adequacy application. The applicant state has to put in its application and produce its law. There is an assessment by a university, and then it goes to the Article 31 and 29 committees. We would have no way of knowing whether it would be different.

The Chairman: That is all from us. It has been extremely helpful. Thank you very much indeed for your evidence. If, on reflection, based on the questions that we have asked you, there is anything that you wish to submit to us in writing, please feel free to do so, but we are very grateful to you for your time this morning. Thank you very much indeed.