

WEDNESDAY 20 FEBRUARY 2008

---

Present

Bledisloe, V  
Goodlad, L (Chairman)  
Lyell of Markyate, L  
Morris of Aberavon, L  
Norton of Louth, L  
O’Cathain, B  
Peston, L  
Quin, B  
Rodgers of Quarry Bank, L  
Rowlands, L  
Smith of Clifton, L  
Woolf, L

---

Witnesses: **Mr Philip Virgo**, Secretary General, EURIM (the European Information Society Group), **Mr Toby Stevens**, Director, Enterprise Privacy Group, and **Mr Mike Bradford**, Director of Regulatory and Consumer Affairs, Experian on the Surveillance Inquiry, examined.

**Q1 Chairman:** Gentlemen, good morning. Thank you very much indeed for coming. Welcome to the Committee. My apologies for keeping you waiting for a bit. We are not being televised but we are being recorded, so could I ask you to state your names and organisations for the record?

**Mr Stevens:** Toby Stevens, Enterprise Privacy Group.

**Mr Bradford:** Mike Bradford, Experian.

**Mr Virgo:** Philip Virgo, EURIM.

**Q2 Chairman:** Thank you very much indeed. Would you, before we start questions, like to make an opening statement?

**Mr Stevens:** Very briefly. Thank you. My Lord Chairman, I am the Director of the Enterprise Privacy Group which is a think-tank for public authorities, private companies and academics to collaborate and resolve issues arising from the management of personal information. We meet regularly to develop shared intellectual property in the space which we then also share appropriately to inform the public debate. The opinions I give today are my own and do not necessarily reflect those of my group's member organisations.

**Q3 Baroness O'Cathain:** Could I ask how that is funded?

**Mr Stevens:** We are privately funded by member subscriptions.

**Q4 Chairman:** Thank you.

**Mr Bradford:** My Lord Chairman, I am Mike Bradford, my role within Experian is Director of Regulatory and Consumer Affairs, so my role is effectively to ensure that Experian complies with both the letter and the spirit of all data-related legislation, privacy and so on. Experian is a plc listed in the FTSE-100, employing 15,500 people across the globe. One of our principle activities is that of a credit bureau or credit reference agency but, more accurately, we provide private and public sector clients with data and solutions to enable them to build citizen or consumer relationships. We also do a lot of work with consumer groups and consumers directly to try to break down the concerns or myths they may have about the uses of personal data.

**Mr Virgo:** I am Philip Virgo, Secretary General of EURIM. EURIM brings together politicians, officials, industry to look at difficult policy issues that cross organisational boundaries. Originally it was, I suppose, a spin-off from the Parliamentary IT Committee but it was set up very much legally, financially and everything else separately, but it has a very heavy overlap of membership. I think our accounts are on the website, together with full

details of our governance. It is a company limited by guarantee, so it is not a registered all-party group but in many respects it behaves as though it was.

**Q5 Chairman:** Apart from data security, how seriously you think the information technology industry and its customers take privacy and human rights issues? How do your organisations work to improve the awareness and behaviour of the industry and its customers in the development of information systems that collect and process individuals' data?

**Mr Virgo:** I am asked to lead on this. We discussed it outside. The main thing is that the IT industry and its customers are as confused about privacy and human rights issues as the whole of the rest of society, including policy-makers and Parliament. There is a great raft of pressures in the IT industry of “put your data on social networks”, “give us your data” and so on, so there is one group which does not appear to value these things at all and about five million of the population have put things on to those websites that one would never dream of putting on if you were concerned about privacy, and then there are those who take the privacy and confidentiality of their customers extremely seriously, but every regulator in sight wants them to record every transaction or communication and make it available for posterity in case it is needed. We really do have an extremely confused situation, where the IT industry is trying to meet the demands of those who are serious about trying to meet the needs of their customers, including government, regulators and everybody else, who are extremely confused as to what the priorities are and what they should be doing.

**Mr Bradford:** On a slightly different tack but nonetheless agreeing with my colleague, as one drills into organisations, the awareness of IT privacy issues, human rights issues, is very dependent on where that IT function sits within an organisation. If you look at some sectors, some immature organisations, you will still see the IT function and the IT specialist almost sitting in a silo. In more innovative businesses or more mature businesses, the most successful positioning of IT is very much allied to the business, so, as and when they are

looking at systems development and so on, it is an integral part of what the business as a whole is doing, not just IT. Looking at certainly some big private sector organisations, you will find IT is very much a business facilitator and not merely a separate function in its own right.

**Q6 Chairman:** Is the industry interested in incorporating privacy-enhancing technologies in its products? Is it already doing so?

**Mr Stevens:** My Lord Chairman, firstly the commonly used expression “privacy-enhancing technologies” is one with which I am not entirely comfortable. I prefer to refer to “privacy-protecting technologies” since privacy enhancement suggests that you are being given something back that you were not necessarily entitled to in the first place. Certainly within our organisation we tend to talk more about privacy-protecting technologies. The industry is focused very hard on this. The problem that they often seem to stumble up against is the lack of a common framework, a common language, a common understanding of what the problems are and what the desired outcomes look like. The Engineering and Physical Science Research Council has kicked off some excellent work in that space to try to understand some of the more fundamental privacy issues faced by corporates, so there is a great deal of work happening. To date, most of the privacy-enhancing technology programmes that we have seen over recent years have failed, either due to lack of interoperability between those that roll them out or a lack of perceived consumer demand. That does not mean it is not there, but the consumers have failed to understand what it is they are being offered.

**Mr Virgo:** To build on that point, there are a lot of technologies about, some of which work, and they just have not been deployed for that reason. The bigger issue is not the technologies themselves. A really good secure technology is lethal if you now roll it out and give 400,000 people access to the data over it. The technologies are only there to support people processes. Basically, if you are going to give large numbers of people access to data over a secure

technology, you are basically assuming that all the staff of the NHS are going to follow security processes rather better than the radio operators of the Wehrmacht and the Luftwaffe and the rest of it. I was trained as a Cold War radio operator and, basically, I would regard most of the systems, even if we were operating under military discipline, as unusable and insecure if you rolled out those numbers, and in a civilian environment the things have not been thought through. If you want security, it is either hierarchies or rings of trust, and it is broken up. Mass market systems and security are extremely difficult to reconcile.

**Q7 Chairman:** Perhaps I could ask Mr Stevens and Mr Virgo whether the training of information technology professionals includes consciousness of privacy considerations and what your organisations are doing towards that objective, if anything?

**Mr Virgo:** Speaking as a former Vice-Chairman of the Professional Board of the British Computer Society, it is included in the exams and the courses but I have to say that most of the students skip that section because there are not enough marks on it and it is worthy but boring. It is the issue of getting people to appreciate treating the data of your customers as though it is your own and building security right into the core of the system, so that you deal with us because we are more secure than they are down the road. Until that is part of the marketing requirement, then it will not be taken that seriously. That is a people issue, not an IT industry issue. It is an overall organisational thing. The industry responds to the priorities of its customers.

**Q8 Lord Lyell of Markyate:** Could I cut back to a question of which I am afraid you have not had notice but which is pretty fundamental: article 8 of the ECHR says that there should be protection of people's private and family life and so on. Are there some things which you could enumerate now which you would regard as utterly beyond the pale? If so, when being exercised by whom and in what circumstances? Such as, for example, "bugging". We have

heard something about “smart dust” – I do not know whether it really exists but apparently it means you can listen to almost everybody’s conversation by leaving this invisible stuff around – or there is hacking into people’s personal computers to see what their interests and predilections might be in order to use them for some embarrassing purpose. What is beyond the pale in your view?

**Mr Bradford:** The two examples you have given there are perfect examples of subjectively what I would consider to be beyond the pale. When I look at the way my own organisation uses data – and I guess my role in Experian is to act as the emotional and legal policeman for that – we will look very carefully at the legitimacy of what perhaps a client requires the data for. It is very much around what the Data Protection Act enables us to do. We will look at the public benefit element of that, which is not like the two examples you have given but is very much: “Is there a real citizen-centric benefit to that person having their data accessed?” or, the other way around – which is more the law enforcement end of things – “Is there a greater public benefit in an individual’s data being accessed even though that individual may not have given their agreement to that?” I think the cut-off is somewhere in there.

**Mr Stevens:** Just to build on those comments, with which I completely agree, the two issues here that are very important to understand what is beyond the pale are, firstly, context. What for any one of us may seem a perfectly reasonable step, to another may seem totally unacceptable. The old example, of course, is that of a battered wife who has fled her husband: at that moment her new home address is an incredibly sensitive piece of personal information from her perspective. We go beyond the pale when we use disproportionate solutions in the handling of data; in other words, where for the individual concerned the use of that data is not proportionate to the problem or the social need.

**Q9 Lord Peston:** Are you saying that in the real world, to take the example of the battered wife, who gets a new credit card and the credit card will have her new address on it, that there is a way into the credit card system so that someone could access her address?

**Mr Stevens:** Unfortunately, it is the sin that dare not speak its name: insider fraud.

**Q10 Lord Peston:** I am still asking about the practice. A person who wanted to go and batter his wife has to find the insider and then go through this whole rigmarole. Is he not better off getting another wife and battering her? I mean, I really do think that a lot of the examples we are quoted do not seem to bear any resemblance to the real world. Can you give us an example? If I go into Sainsbury's and use my Visa card, which contains a lot of information, what process would then enable someone to get from my purchase to me? I would have thought the expense was massive.

**Mr Bradford:** My Lord Chairman, perhaps I might tackle that, bearing in mind my own business is very much part and parcel of providing clients with personal data. The fundamental in my own business, of any data-based organisation, is for us to be compliant and for us to retain consumer and client trust. We can only provide information that complies with the Data Protection Act. Fundamentally, unless that particular individual is aware of what their personal data may be used for and by whom, then any use of that data – and that could include, say, for example, using a store card and monitoring what your purchases are – if you had not previously been made aware that that was how you were going to have your data used would be a fundamental breach of the Act.

**Lord Peston:** That is really my point. The store would be looking at data of this sort to classify it and make it useful to them economically. Does the store have any interest in its individual clients?

**Chairman:** I am going to call Lady Quin next, because I think we have to move on, but I would just mention that my wife, two weeks ago, had a birthday card from Sainsbury's!

**Q11 Baroness Quin:** I am going to go back to something you started to address earlier on. It is about the factors which currently inhibit or encourage further development of PET – or perhaps I should say PPT – solutions, in particular what seems to me the difficulty of striking a balance between the need in large organisations to share information and at the same time build in fire walls and protection. In particular, are government procurement specifications sufficiently helpful in ensuring that data protection is designed into new systems?

**Mr Virgo:** It is before the procurement. It is the original concept of the system and the way in which it is designed and intended. The damage is done before the procurement takes place. There are assumptions made about the security of the people who are going to run the system which are not borne out in practice. One takes the very simple contrast: most of the Experiens of this world vet all their staff and have rings of trust and the rest of it; but various government departments are tasked to meet quotas of recruits from various local communities. There is the example of the Immigration and Passport Service having to meet its quotas of recruitment in Croydon and that meant that all sorts of people were not vetted or checked and you have illegal immigrants ending up working within the system. That happens before anything has gone out to procurement, so, whatever you did in the procurement, you would actually have the “insiders” within the system. That is why I say secure technology operated by insecure people is lethal and, in that kind of example, you have the situation within the immigrant communities of forced marriages being policed and, if they try to escape, the extended relatives, who have access to the system for their job within the public sector, will help do the tracking and tracing and so on. There was the recent case of a tussle over a car-parking place in Asda resulting in the wife ringing her husband, who rang a policeman friend, who then got the address of the pensioner, and they then went and threw a brick through his window and he died of a heart attack. No privacy-enhancing technology

would address that kind of thing. The people processes are what you have to look at in that context.

**Q12 Baroness O’Cathain:** Does that mean that it could not ever be safe or that there is a sort of failure right at the beginning to specify correctly the whole system? Going straight on from that, is that not what has happened with government projects, and not only government projects but other big company projects, over the last ten years?

**Mr Virgo:** Exactly. It is the specification right at the very beginning. In government projects there is a systemic problem and the systemic problem is essentially that the policy is conceived by a set of advisors and a minister, it then starts gathering life and, on average – and I will not say this is statistically solid – between the policy being formed and the legislation going to the House there will be one change of officials, then between the primary legislation and the statutory instruments to implement it there will be two changes of minister and another change of officials, then you go through to the procurement. That churn means that whatever gets implemented is not the original policy and the specification gets compromised and corrupted along that process.

**Mr Stevens:** My Lord Chairman, may I add to that point – with which, again, I fully agree. For a corporate entity, security and privacy are the same thing: it is simply the nature of the data that they are handling. It is purely for the data subject that the privacy becomes a sensitive issue. I would certainly agree that government procurement does not reflect good privacy practice in general. This is not necessarily the fault of any one individual. We do see a problem that the cheapest way to implement transformational government objectives is to aggregate or “zipper” data into larger databases rather than taking the more complex but privacy protecting route of federated or compartmented databases – which, just as with a hole within a ship, will prevent leakage between the different areas – where we can manage the large user base without giving them access to everything.

**Q13 Lord Peston:** My question is about organisations promoting privacy impact assessments. I had assumed that most things like the Lord Chairman's wife getting a birthday card or the vouchers we get every month from Marks & Spencer, proportionate to how much we spend, and also from Tesco, were all done automatically by a computer and that no human beings were involved at all. Indeed, if you take the view, then you cannot have any privacy protection at all – after all, the person who posts the letters from Marks & Spencer can look through the whole list of letters and see some names. In promoting privacy impact assessments, I take it you are not asking for the moon.

**Mr Bradford:** Without knowing the ins and outs of that particular organisation, I would suspect the way that will work is that, at the time you opened up the relationship with that particular supplier, be it Sainsbury's or whoever, there will be what we call a "fair obtaining clause" that will tell you what your data may be used for, by whom and so on, and you will, strictly speaking, be given the ability to agree to that or potentially not to agree to it. If you decide, "Yes, I am happy for this to happen" ----

**Q14 Lord Peston:** Who is "you" in this context?

**Mr Bradford:** As the consumer.

**Q15 Lord Peston:** It would never occur to the consumer. It never occurred to me until the Lord Chairman mentioned his wife's birthday card that these cases arise. One must want to know about the organisation and its responsibilities. You cannot expect me every time I go shopping to do a privacy impact assessment.

**Mr Bradford:** The two are slightly disconnected. When you go into an organisation as a customer and you are going to transact or open a credit card or whatever you are going to do, there will be or should be a full explanation given to that consumer of what their data will be used for. One of the things may be: "We may use your data to contact you for future offers

that may be of interest.” That is, if you like, the obligation of certainly the organisation. As to a privacy impact assessment, to move on to that, perhaps I could draw again on my own role in my own organisation. Clearly we hold a lot of information which we have obtained fairly and lawfully within the meaning of the Data Protection Act. Consumers know their data is held within Experian and there are ways that we do that. When we come to look at designing a new product for a client to benefit a consumer, then we can only do with that data what the consumer has already been told. If, for example, the consumer has given their agreement that their data may be used, typically in the credit environment, for assessing a credit application, then the only way we can use that data is to help the client assess a credit application. We cannot take it out of there and develop, if you like, a birthday card list for a client so that all our wives and loved ones can get birthday cards. My job in the organisation is to make sure that every product that we design hits or meets that criteria, both the legal criteria of what we can and cannot legally do and, also, if you like, the reputation and emotional criteria of what we should and should not be doing. That is the way it would work in my own organisation.

**Q16 Lord Peston:** Just to summarise, the answer to my question is yes.

*Mr Bradford:* If I could remember the question I would answer.

**Q17 Lord Peston:** The question is: Do you promote the use of privacy impact assessments?

*Mr Bradford:* Yes, we certainly do. We have to, yes.

**Q18 Lord Lyell of Markyate:** Some birthday cards may be legitimate but less welcome.

*Mr Bradford:* Absolutely.

**Lord Lyell of Markyate:** My next birthday will be 70 and I am expecting some letter or card from the DVLA at Swansea to tell me that I must now apply for an annual driving licence. That seems, albeit unhappy, to be legitimate.

**Q19 Lord Morris of Aberavon:** Could I ask about the ever-advancing development of the technical side of IT. How aware are the policy-makers and parliamentarians of this and of the social and citizenship issues of the surveillance society? How can we compare the awareness of policy-makers with that of other countries?

**Mr Virgo:** Having spent 25 years or so as piggy-in-the-middle in this area of trying to improve understanding between politicians and the IT industry, my honest answer is that the politicians understand the IT industry and the implications of technology rather better than the IT professionals understand politics and their responsibilities as professionals for trying to educate policy-makers about the potential implications of their technologies. It is not so much the theoretical technologies as to what might be possible, but what can actually be delivered with the technologies you have which are tested, which are working, and the people you have to deliver it. An awful lot of assumptions about technology cannot be delivered with the people, the time and the budgets you have. There was a meeting of very senior software engineers at what was then the Institute of Electrical Engineers. The conclusion was that the main protection for our privacy is that most of the surveillance technologies do not work and even those which do do not interoperate, and therefore an awful lot of the threats are theoretical rather than real.

**Q20 Lord Norton of Louth:** One of the issues you touched on earlier relates to the legislation process itself and whether it is fit for purpose in terms of its capacity to take into account privacy issues. Do you see any problems with the process as it presently operates?

**Mr Virgo:** There are a lot of problems. EURIM were heavily involved trying to do damage limitation on the original Regulation of Investigatory Powers Act, beginning with the Alison Halford case and IOCA review onwards, trying to get people to understand where each other was coming from. We then used that experience to try to help what became the scrutiny process for the Ofcom Bill and, in that, working with the bill team and the clerks of the House to try to do an exercise to identify the areas that were going to be relatively easy and the areas that were going to be difficult, so that they could plan and schedule what became the pre-consultation process before a joint committee of the Lords and the Commons, to make best use of the time to identify the things that were going to cause problems, so that the legislative process itself was relatively smooth. Observers have said that on a bill of that complexity it saved about 400 amendments. That bill would have had a couple of thousand and it went through with about 1400. Those really changed bells and whistles and made the implementation smoother; they did not really change anything that the officials had not already wanted to do and government wanted to do anyway. I can provide all sorts of documentation as to how that process worked – because I think it was a very good model and we spent a lot of time trying to make it happen – but there are limitations to it. I was consulting some of our parliamentary members, particularly one of the committee chairmen and he was saying, “Don’t over-egg what you have achieved. All you did was make the process run smoother; you did not actually change anything.”

**Q21 Lord Morris of Aberavon:** That was premised on there being pre-legislative scrutiny anyway.

**Mr Virgo:** Exactly.

**Q22 Lord Norton of Louth:** And that was exceptional.

**Mr Virgo:** It was, indeed.

**Q23 Lord Norton of Louth:** Is there anything that could be done on a more systematic basis and is there anything we can learn from overseas? In other words, is this a common problem?

*Mr Virgo:* It is, indeed, a common problem.

*Mr Stevens:* In the past five or six years, in particular, this space has been dominated by the tension between national security and citizen privacy, and national security in many bills, in my personal opinion, has been used to browbeat privacy concerns. Unfortunately, good privacy often results in much better data quality because it shows respect for the integrity and the handling of that data. We are seeing examples now of systems which are not delivering what was wished for because they were pushed through on a national security agenda when, in fact, a citizen-centric, higher quality solution would have been achieved if we had looked at the bigger picture.

**Q24 Lord Norton of Louth:** How does one address that? Is it a procedural matter? Is it essentially a matter of awareness, so that you get that consistency, if you like the priority, given the ----

*Mr Virgo:* It is awareness and prioritisation. The Belgian system, with its checks and balances and the rest of it, is extremely good but I think it is good because Belgium is a small but intensely federated country – more ministers per kilometre than anywhere else in the world. It also has this tradition of being occupied and the files being taken over by the Gestapo. That affects the reasoning why the Dutch and the Belgians particularly have much stronger and more solid and robust processes in this area, because of that legacy of mistrust.

**Q25 Lord Norton of Louth:** Is there anything we can learn from that in terms of process?

*Mr Virgo:* I do not think there is anything we can learn from the processes of other legislatures. In all honesty I would have to think about that rather more.

**Mr Stevens:** My Lord Chairman, may I add the example of Germany, where we have a written constitution that prevents the aggregating of citizen data at a federal level; where the government respects that to the point that they are able, in one example, to prevent the German state railway from issuing its own credit card. It was their own government that they stopped from doing that because it would have meant sending data overseas and aggregating it in a way that they were not comfortable with.

**Q26 Lord Rowlands:** Your last reply touches on the question I was about to ask you. We are a constitution committee – not just a public policy committee but a constitution committee. In a recent international survey of privacy laws right across the globe, we came out very negatively on constitutional safeguards. As three people who are heavily involved in all this movement information, et cetera, do you have any suggestions about what constitutional safeguards are required to bring this up to some better norm?

**Mr Bradford:** There is almost a flip side to what we are talking about. The word in the question “surveillance” society is something that concerns me. In our geographies, which are across Europe and globally, ironically, although the UK may be perceived as having weak constitutional protection around data, we need to be aware that by constantly referring to a surveillance society we are increasing the concerns of individuals – and I would argue, in many cases, potentially unnecessarily. At the end of the day, good privacy protection is designed to protect good citizens, and the very people that we end up not protecting by being almost over complex with the checks and balances we put in are the people we possibly would rather we did not try to protect. Without being too revolutionary about it, I think we need to be very careful that data breach reporting, uses of data, does not play to a mass gallery of almost privacy paranoia but plays to something that is a legitimate balance of privacy protection versus public interest. To go to that point specifically, I see how personal data are used across the EU. The EU is meant to be operating, for example, under one single

European Data Protection Directive. It got 27 different interpretations of that Directive in 27 different countries. You could argue, looking at it commercially, rather than, say, from a strict privacy point of view: Is the best country that which interprets it in its most strict way? I would argue not. I would argue that if you look at the UK, which is constantly quoted by the World Bank from a credit perspective as balancing privacy interests with the ability to get credit – and you could argue is there an indebtedness issue and so on but we have hopefully parked that – then in the UK, which accounts for over 30 per cent of EU lending, we have a regulatory and commercial environment that allows consumers to use their data for their own benefit. I think the bigger challenge is around consumers starting to think – maybe the public sector: “What is my data being used for? Is it Big Brother?” I know that perhaps later we will be looking at ID cards and I think the bit we have to address is not so much process but one of trust and if consumers do not trust what their data is used for.

**Q27 Lord Rowlands:** You quoted the German example which was a constitutional safeguard. Are there any constitutional safeguards we should be considering?

**Mr Stevens:** My Lord Chairman, if I were able to propose a single safeguard it would be for an enhanced level of privacy controls over data where that is collected in a non consensual fashion. We pay taxes, therefore we expect the Treasury, the Revenue, to be able to gather information about fellow citizens to collect their taxes, so we cannot opt out of their databases. Nor can we take our business to another revenue if we do not like the one we are dealing with. Those organisations that are above that consent should be bound by a higher moral duty and subject to an enhanced level of inspection. The Cabinet Office and the CESG division of GCHQ provide the Manual of Protective Security and the various government memoranda/guidelines for protecting the security of data. It would be fascinating to see an equivalent function for personal data that is responsible for ensuring that the correct privacy

impact assessments are carried out, and that is the advocate for the citizen where non consensual data is processed.

**Mr Virgo:** There is an approach which we looked at but we never carried forward, not because we thought it was wrong but because the group concerned just stopped working. Essentially, we have far too many regulators, commissioners and so on in this area. We have an overload of governance and the effect is lack of confidence and no governance. The approach was, in fact, that all of these commissioners and all the rest of it should be replaced by a joint committee of both Houses. Given time pressures on the other Place, that would effectively mean it would be a committee of your Lordships who would have to be doing the work on it, but to have that governance open and transparent. At the moment, we have all sorts of officials who have the status of a chief constable and you then look and you find this is a functionary somewhere in the Home Office or the Ministry of Justice or what-have-you who has the “status of” and when you look at this from the point of view of, let us say, legal counsel to an American bank handling Arab and overseas clients in London, your reaction, as in the case of RIPA was, we move the files out of the UK. The dealers may be in the UK but the files and keys are sitting under Swiss or offshore legislation or they are split. “We do not trust this governance because we cannot understand it and our counsel tells us that it is different from what the minister said it was in the House.”

**Q28 Lord Lyell of Markyate:** This is extraordinarily interesting. Could I just jog back to what Mr Stevens was saying about heavy-handed national security powers working against privacy-centric ideas. I think the point you were making was that if they had tried to be more privacy-centric, they would have got more useful data. Can you give an example or two of that?

**Mr Stevens:** To give a hypothetical example: obviously the polemic that has arisen from the national identity scheme has caused a great deal of debate over the past few years and this, in

my opinion, is because the citizen cannot see the day-to-day benefit to them. National security/illegal immigration for most of us do not impact us on a day-to-day basis. As long as they are working they remain invisible. However, if we were to adopt the process used by many other countries to offer citizen-centric services to deliver true transformational government, to integrate business, I could, for example, enrol for a national identity card with a bank which happens to be part of the Government's broader scheme and then would willingly want to risk far more data with them because I would be able to get my own commercial value from that. The problem that we are looking at here is this lack of transparency in these schemes and where commerce has not been fully engaged from the start. Perhaps I could stress, My Lord Chairman, that is not a plea from my members in any way, shape or form but a personal opinion, and there would still be a lot of scope to explore schemes such as those in Hong Kong, Belgium, emerging in the likes of Canada, where they are taking this approach.

**Q29 Lord Lyell of Markyate:** Thank you. Is it possible to give a non hypothetical example? Because I am struggling.

**Mr Stevens:** Could I respond on that after please, My Lord Chairman.

**Chairman:** Yes.

**Q30 Lord Woolf:** What are your collective views of the efficiency of our current regulatory laws and other frameworks for limiting surveillance and protecting privacy, whether in the UK or in the EU?

**Mr Virgo:** I have with me a paper which was updated at my request for another purpose, particularly on our data retention requirements, because retained data is vulnerable data. We have retentions running from four days to a century under a whole raft of different legislative requirements, some going back to the First World War, others recent, and all of those

retentions are, “We might need it because a regulator might need access” or “There might be statutory access” and that data is either properly managed (recycled and circulated so that it can be accessed) and therefore is vulnerable to abuse by those who are doing the management – and that is a very expensive process – or it is put into a long-lasting medium, down a secure coal mine, and is probably unreadable within a couple of years because computer operating systems have moved on, different microfiche readers and so on. There is a department of the University of London which is essentially a museum whose prime line of business is working with The National Archives rebuilding equipment to recover stuff from those obsolete technologies. It is a muddle and it is a confusion. It is because regulator upon regulator upon regulator says either “It is forbidden” or “It is mandatory” and has different requirements. They are never brought together.

**Q31 Baroness O’Cathain:** If you have these regulators, regulators, regulators, are they operating on a silo basis? Do they never talk to each other?

*Mr Virgo:* Some sporadically talk to each other.

**Q32 Baroness O’Cathain:** There is no requirement for them to talk to each other?

*Mr Virgo:* There is no requirement. The only organisation I have seen that has a coherent way of bringing them together is Lloyd’s of London for the insurance regulators, which regularly runs courses and conferences for regulators, with extremely good hospitality, and they all turn up because they meet each other and that is about the only occasion they do meet each other.

**Q33 Baroness O’Cathain:** Is there a need for an overarching regulator?

*Mr Virgo:* Yes.

**Q34 Baroness O’Cathain:** Rather than a joint committee of both Houses or the House of Lords Committee.

**Mr Virgo:** I would not say an overarching regulator because at that point you suddenly get hierarchies upon hierarchies upon hierarchies.

**Q35 Baroness O’Cathain:** Or silos.

**Mr Virgo:** You need a process that will bring about rationalisation and break open the silos over time.

**Q36 Lord Woolf:** It may be that you cannot answer what I was specifically putting to you: Do we need more legislation and, for an example, would you like to see changes in the Data Protection Act or the powers or the role of the Information Commissioner?

**Mr Bradford:** There are some very good things about the DPA but the one good thing in this context is that its design should be sufficiently dynamic to move forward with changing times, so if you look at the Data Protection Act it is virtually IT agnostic. It does not specify minimum requirements for this, that and the other, but it would put the onus on any organisation, be it public or private sector, to defend any data breach or whatever in line with the current best practice for information security technology, be it ISO or whatever. I think there are areas possibly within the Data Protection Act. In a commercial arena, basically it is our bible and everything we do with data must comply with that, and certainly on a quarterly basis we will be having discussions with Richard Thomas’s office around what we are doing and what we are looking to do and so on. I think, though, in other sectors – and we have seen examples of this – there is far less clarity around what they can and cannot do and we have seen that leading to some rather unfortunate incidents where perhaps people do not think they can do something when they can. Whether it needs to be changed or whether there needs to

be clarity around how it can be applied and interpreted, I would say it is the latter that could be addressed, not the actual legislation.

**Q37 Lord Woolf:** More information about what the legislation requires, is what you are saying?

**Mr Bradford:** Yes.

**Q38 Lord Woolf:** I think you are content with the legislation.

**Mr Stevens:** My Lord Chairman, to add to that, in my opinion the Data Protection Act, whilst it is a commendable piece of legislation, does of course operate as a business enabler to allow the transfer of data between organisations, individuals and nation states. The problem that we suffer from in the UK is an Information Commissioner's office that is not adequately resourced to keep up with the legislative burden being placed upon it. In particular, as a result, they have to remain focused on promoting data protection awareness rather than enforcing data protection because that requires such a great resource intensiveness for them. The majority of organisations in the private sector, if they were to choose to do so, could disregard most of its requirements, knowing that the outcome will probably be cheaper than the cost of compliance. Within the public sector we see many cases of non compliance resulting in no penalty at all for the individuals affected, where there is little point in transferring taxpayers' funds from one body to another in the form of a fine.

**Mr Bradford:** Perhaps I could pick up on a point which I think is very important. While the cost of non compliance in terms of censure may be potentially minimal, for a commercial organisation, especially a plc, to end up with a headline that says "There has been a data breach at Company X" is a phenomenal cost to the business. I do not think the deterrent need be on the small print; the deterrent is in the breach which will potentially be reported.

**Mr Stevens:** I would totally agree with that.

**Q39 Lord Woolf:** You have already identified the lack of resources for the commissioners. Do you need to see any changes with regard to their powers and their ability to have oversight? In particular, do you see the Regulation of Investigatory Powers Act as being effective in any way?

**Mr Virgo:** Yes. That is an extremely good point, because parts of the Regulation of Investigatory Powers Act are extremely good – the bits that are to do with the regulation of investigatory powers – and they need to be greatly strengthened. When the bill was going through, there was all sorts of stuff about the training and the codes of practice for those who were going to have the surveillance powers, and an awful lot of that training has never happened. Departments which did not train their staff in how to use the powers were supposedly going to lose the powers. That has never happened.

**Q40 Lord Woolf:** That is the enforcement of it.

**Mr Virgo:** It is the enforcement. As with the Information Commissioner, it is the enforcement powers and, particularly, the enforcement powers with regard to the public sector – because, as was said by my colleagues, the private sector is very concerned about its reputation; the public sector does not have to be concerned about reputation because its customers do not have a choice.

**Q41 Lord Woolf:** I glean from your answers generally that there are problems but they are not with regard to the powers that legislation have given or prohibitions that the legislation has imposed.

**Mr Virgo:** When there is a breach of data protection. If I remember correctly, the Department of Transport civil servant who used his access to give names and addresses of cars outside Darley Oaks Farm to animal rights terrorists so they could then follow through had to be done for misprision in public office because nobody could find an alternative piece

of legislation with suitable penalties. And if the individual had been a temp and not in public office, the penalties were derisory. There are issues to do with the penalties for breach which really do need to be brought through and enforced and implemented.

**Q42 Lord Rowlands:** Mr Virgo, I do not think I can let you get away with such a sweeping statement about the public sector that you have just made. There are staff in the NHS who are equally conscientious and as determined. You seem to give an impression that because you have a monopoly service of one kind you certainly do not care for your customers.

*Mr Virgo:* I am sorry.

**Q43 Lord Rowlands:** I think you should withdraw that ----

*Mr Virgo:* I should indeed because it is the system and the way in which the system operates. You are absolutely right, some of those who are most concerned about data breaches are indeed those in the Health Service. I married into a medical family and they have very strong views on protecting the data of their patients, but they are protecting it, as they see it, against a system and the system is designed by people with particular mindsets. I do apologise for that impression because, you are absolutely right, it was a sweeping statement that I should not have made.

**Q44 Lord Lyell of Markyate:** What you are saying is very pertinent to the Regulatory Enforcement and Sanctions Bill which is going through Parliament. I personally am worried, and I have said it often in the Committee, that we are giving the power to every regulator – and that will go right down to local authority officials themselves – to impose fines. They are called civil penalties but they are effectively fines – which can be enormous but will often be automatic – but may be £1,000 and not variable. I am worried that we are going to see an awful lot of bullying and overkill. I can see that there are worries in data protection that they

have not got enough, but there will not even be court surveillance, true court surveillance, if we go down this route. Has this crossed your desk as a problem?

*Mr Virgo:* This was the thing within the regulation of investigatory powers at a higher level, where industry wanted things to go through the courts and not through administrative procedures. That really is a major concern to industry that it wants things through the courts because that way it has a form of certainty that it does not have if it goes administratively.

**Q45 Lord Lyell of Markyate:** The Hampton Review by the Managing Director of Sainsbury's and the Macrory Report by Professor Macrory are leading in exactly the opposite direction, although we are told that it is all business friendly.

*Mr Virgo:* Those who are involved in information insurance and so on, who are looking for certainty, have one set of views, but this is not an area, I think, where you can say there is a single industry view. There are some things which are cheaper to do and there are others which are more confidence-enhancing. I have to say that certainly all of the meetings in which I have been involved have always been going down a route of: "These things should be open and transparent; they should not be behind closed doors administratively".

**Q46 Baroness O'Cathain:** My question regards the identification of individuals for marketing in commercial organisations and, indeed, for public sector services. These places - we have already dealt with some of them (credit cards et cetera) - involve identity management systems. Are adequate privacy and security safeguards incorporated in them and, if they are, do you think that can be transferred across to the current identity cards project in this country?

*Mr Bradford:* My Lord Chairman, may I start? If look at it from a commercial sector point of view, increasingly (and we saw this with our clients over the last probably six or seven years, in particular with Internet-based transactions) one of the first things a commercial

organisation looking to transact with a consumer would want to do, especially remotely, is to verify, firstly, that there is a Mike Bradford that exists and, secondly, that the consumer at the other end of that telephone or Internet line is the Mike Bradford. Typically, in a commercial organisation what we call the authentication process, which is the, “Is this the Mike Bradford?”, will be carried out with the agreement of that consumer who is looking, at that stage, to transact with this particular organisation. So, they will be informed at the point of transaction, firstly, that what we are going to do, if you are okay with it, is verify that you are who you claim to be (and it is very open, very transparent), and if at that point they say, “No, we do not want you to do that”, then maybe you go into paper proofs and the various other ways of doing things, but certainly in a commercial sector, unless it falls under one of two large but very limited pieces of legislation where there is a legislative requirement to provide data whether or not the consumer agrees to it, any identity management product will be operated with that agreement of the individual, and that is at the point of transaction usually.

**Mr Virgo:** The key point here, though, is in fact this one of informed choice, because far too many systems, even when there is a supposed choice, are: take it or leave it. In the public sector you have either got to give the information and it has got to be shared, or it is forbidden to be shared. There is not the element of choice which says, “If I give you more information, can you process my claim more quickly”, and in the private sector very often there is a catch-all consent, or otherwise, and four pages of small print which may or may not be enforceable. I am trying to remember my business school law course and I cannot remember which legislation and case law applies - unfair clauses, and so on. On the actual issue of being able to choose to give more information in return for a discount voucher, or what have you, different organisations in the private sector deal with this differently. There are some which say, “Give us all this information. We will give you discounts. Oh, and by the way, we will not give it to anybody else except under a court order because we want you to do your

transactions through us.” They then guard that data, because it is giving them an advantage. There are others who try and collect the data and then sell it on. You need to have a choice as to which you are doing.

**Chairman:** Lord Peston. Can I make my traditional Chairman’s appeal for brief replies, because time is marching on?

**Q47 Lord Peston:** Yes. What puzzles me, in a sense, this question, which is of fundamental importance, is the converse of the privacy question. The private sector seems to have cracked it to some degree. Certainly if I engage in online banking, I have to type in some numbers; if I engage in telephone banking I have to give them some numbers; if I go with my credit card now I have to put in some numbers and it seems to work very well, in the sense that I am identifying me as me and then it can all go ahead. What seems to be the mess is the public sector. This anticipates what Lady O’Cathain will go into in more detail. The public sector, having realised that people have to establish, for all sorts of purposes, “This is me”, and then you think, let us have the equivalent, namely an identity card, has produced the most complex thing which no private sector firm would have engaged in anyway, apart from anything else, because of the sheer cost. A private sector firm would not have invented a scheme that would cost billions. Can you comment on that?

**Mr Stevens:** My Lord Chairman (and this also addresses the second part of my Lady’s question earlier), I think the national identity scheme in particular has a very different fundamental requirement from a typical identity management scheme. If we treat credit cards and the very successful credit card networks as a scheme that we all know and trust, those systems tolerate a degree of fraud and it is factored into their business model. Fixing that final bit of fraud would be far too expensive, so it is far better to accept that that will happen. In a national identity scheme which is being used for national security purposes, that small bit of fraud could be the bit that causes the failure of the scheme by failing to identify the wrong

individuals, and so on. I think there is a failure amongst some, and I stress some, policy-makers to understand the difference between, for example, authentication and identification and entitlement. A credit card proves that I am entitled to make this transaction and my PIN number authenticates that I am the genuine holder of this card, but the shopkeeper knows nothing more about me at this stage than my name, and that name is only on there so that I can pick up the correct card from the dresser in the morning and not accidentally come out with one of my wife's credit cards. It does not actually bear any relation to the transaction.

**Q48 Lord Peston:** Why could we not have a national identity card scheme exactly the same? Let us assume it starts as a voluntary scheme, so that anybody who wants to be able to say, "I am me", would simply voluntarily do it and he or she would get a PIN number?

**Mr Virgo:** Provided you accept that, like most of the identity cards around most of the world, it is a low-value, convenient residence card which simply you register with your council when you move in and you are going to pay your taxes and the rest of it, and when you move house it is a one-stop shop change of address. It is the expectations that have been added to that very basic concept that raise hackles.

**Mr Bradford:** My Lord Chairman, the other point about that as well - we touched on it earlier - is the more the citizen looks to use a card like that the greater the trust they must have in how it is being used, or how its data is used behind the scenes. I think that is another piece to crack.

**Q49 Baroness O'Cathain:** The point is, there are other countries that run identity cards, so all three of you must know in depth how those work. Are there any best practices that we could actually recommend should be taken on board here, or is it like so much that we do in this country, we are gold-plating?

**Mr Bradford:** Maybe I can comment on that. If I look at it again, and I look at it from a commercial organisation's perspective, an identity card or an identity token that says, "I am the Mike Bradford", is only as good as the underlying checks and balances you can do before you issue that card. If I look at the UK private sector, unlike some of the EU countries or the States, we do not have access to the data layers that maybe the public sector have that would give you that certainty that you know that Mike Bradford with a national insurance number X, Y Z and a passport number of---. The card is only as good as the checks you can put into it. In the private sector and the public sector those checks would be, I think, far more robust than just one sector looking at it. That would be my point, I guess, that the efficacy of the card is dependent on the underlying data.

**Mr Stevens:** My Lord Chairman, there are a number changes that one could suggest, but for the sake of brevity if I may point the Committee at two areas. The first is to highlight the work that Microsoft has done in this space on the laws of identity by their chief architect. For example, one of those would be not using the same identifier for different purposes; so not using a national identity number for multiple applications, which would permit different agencies to zipper up data and build a broader view of the individual than they may be entitled to. The second one, to reflect my colleague's comment there, is rather than looking at other countries' identity schemes to look at the private sector and the trust that the likes, for example, of EBay have created in their reputational identity schemes, where a consumer can very quickly make a judgment about the individual that they are about to make a transaction with and decide whether it is safe or not. In my experience it works very well indeed. So, the reputational trust model to which Mr Bradford just referred might be one that would be fascinating in an identity scheme.

**Q50 Baroness O’Cathain:** Can I just ask a very quick supplementary. To your knowledge, are the Government’s people who are looking at the future of identity cards in this country aware of the points that you have been making or even thinking along those lines?

**Mr Bradford:** Certainly in discussions we have had, Lord Chairman, they should be aware.

**Q51 Baroness O’Cathain:** But they are not necessarily buying into it?

**Mr Bradford:** I rest my case.

**Mr Virgo:** I would simply say that on Thursday we have yet another meeting which is basically trying to inform those looking at governments’ identity management schemes, plural, of which the identity card is only one, about the experiences of the private sector around the world in dealing with other governments on identity management, because there are lots and lots of ways of doing it, both public and private sector, they have been around a very long time (thousands of years in fact), they have transitioned onto electronic media, and so on, but there is a great deal of it about and, yes, they are, indeed, looking at other parts of the world and other experiences, I think mainly because of the pressures they have been placed under.

**Q52 Baroness O’Cathain:** The Enterprise Privacy Group has been eager to develop a “business case” for privacy, which may be somewhat different from cases that could be developed on ethical, philosophical or social grounds. Can you explain the business case very briefly, because I know we are running out of time? Why do you think it is an important adjunct?

**Mr Stevens:** Very briefly, our hypothesis here, because it is early days in this piece of work, is that there is no duty upon a private company to offer privacy. They have a compliance duty for data protection, human rights and related laws. There may be a commercial imperative to manage their customers correctly, reduce fraud, protect security, but *per se* their shareholders

have not tasked them with protecting privacy. We believe that privacy is, in fact, a secondary benefit to the consumer arising from good commercial practice, and that is the philosophy that we are now exploring in our work.

**Q53 Baroness O’Cathain:** Of course that is different when it comes to government?

*Mr Stevens:* Government, where we are particularly into non-consensual or monopolistic areas.

**Q54 Baroness O’Cathain:** And you are bound to be absolutely sure about privacy?

*Mr Stevens:* Yes, that is correct. So, that model at this stage is not the one we will explore; that is further down the line of our work.

**Q55 Lord Rodgers of Quarry Bank:** Experian says it has “a leadership position as the trusted steward of often sensitive information and we have an obligation to protect this”. I assume, because I do not wholly understand the organisation, that they have to also take care of its shareholders. It is not a voluntary body; it is there to make money. I ask that really because, given that you collect and you process vast quantities of personal information of the kind we have been discussing, why should we have confidence in your stewardship or, whatever we might call it, custodianship?

*Mr Bradford:* It is certainly not something we would take as read. I think the expectation is because (a) of what we have to do with information and collect it from a data protection perspective, (b) the significant investment we make in compliance and in working with the Information Commissioner’s office, (c) in the work that we actually do directly with consumers. We have a specific function whose job it is to work closely with the National Consumers Council, with Citizens Advice, and we have an area in our business with over 250 people whose job it is to work directly with consumers - not commercial businesses, not our

commercial clients, but with consumers - and to try and help them understand the information we hold, why we hold it fairly and securely and any issues they may have with their data, how they can go around looking to protect that, in particular in the area of fraud, credit card fraud and victims of fraud. We advise our consumers, if that very unfortunate situation occurs, how they can manage their way through that. The very short answer, if I can abbreviate it, is that over a number of years we have tried to build this trust collateral externally, and it is something that will be in the commercial or public sector organisation. The big learning out of that is it takes a long time to build but it does not take long to lose, and I think, looking at ID cards and uses of ID cards, you have to build that reputational and trust collateral first before people have trust in doing business with you.

**Q56 Viscount Bledisloe:** Mr Bradford, it is in the interests of your organisation to collect as much information as it possibly can on people and to disseminate that to as large a number of companies as they can persuade to take it. Is that right?

*Mr Bradford:* Yes.

**Q57 Viscount Bledisloe:** I am not suggesting you are doing anything unethical. That is the main purpose.

*Mr Bradford:* With the agreement of the individuals.

**Q58 Viscount Bledisloe:** That is what I want to know.

*Mr Bradford:* It is not unilateral use of data.

**Q59 Viscount Bledisloe:** Does the individual actually know that information is being passed to you, does he have any opportunity to correct it or to comment on it and would he be happy that, in fact, this information about him is being disseminated worldwide?

**Mr Bradford:** I think we are back at the last point, but if I can give you a very quick working example of how a typical piece of Experian data would be used. When my colleague applies for a credit card, he goes to a credit card organisation and they will say at that point, “We will undertake a search with a credit reference agency”, Experian or the two others in the UK, “(a) to check the validity of your application, to check who you say you are, and, if that application is successful, we will also share data on how you perform that account with other lenders.” At that point there are a number of choices the individual can make. They can decide not to go ahead with the transaction, but from a consent perspective those three checks are considered in the UK to be a reasonable balance, if you lack a trade-off, for that person going forward with that transaction. At the end of the day, it actually helps that person get further credit lines because a good payer, if you like, when somebody else searches that individual, will be shown to have a good track record. So your agreement in that process is such that the data comes into Experian with your agreement; the next time you wish to make a credit application you have the same dialogue with another credit card issuer, who will then open up the Experian data. We are not sitting there unilaterally handing data out, the data is accessed at the point you apply for rental services with a third party organisation. In terms of correction, to go on to that point, Experian issues over one and a half million credit reports a year to consumers. They have a statutory right to ask the credit bureau for their credit report. We actually go further than that and facilitate that over the Internet, online and through partners. So, again, part of our consumer affairs function is to make sure that consumers know where their data is, how they can make sure it is accurate and how they can work with us if they find it is not accurate.

**Q60 Viscount Bledisloe:** You are saying that in some way, when I first take out my credit card, I have consented to them passing the information around, though I had no idea I was doing so, even though I happen to be a lawyer?

**Mr Bradford:** What will happen at that point, and again the Information Commissioner has been very involved in this and I believe EURIM have also commented recently, to use the analogy again, is that on every credit card application there are what are called fair obtaining clauses, and lenders are meant to give some problems to the wording, but legally these will be telling you exactly what your information may be used for, and they will be on those application forms. One thing we have to check and balance within Experian is, before we allow a lender access to our credit bureau, I will have sight of that lender's current credit application form to ensure that I am comfortable that it gives us, as the second party in the process, the ability to take that data. That is the process that it works on.

**Q61 Viscount Bledisloe:** Then I have a row with that card company because I think that they have overcharged me or something like that, I refuse to pay the outstanding balance and I stop using that card. When you are told, "Here is the money which he has not paid", do you find out? Are you told that it is because I have a legitimate complaint, or what I think is legitimate?

**Mr Bradford:** The safeguard for the consumer there, again, bearing in mind the priority we give to ensuring that consumers are aware that they can access their credit report, is that you could actually put a comment on your credit report, which any other lender will see subsequent to that. When it is sitting in a credit bureau the data is inert, no one is looking at it. The only time that that missed payment would be seen is if you were to make another credit application, and you have the right to put a comment against that to say, "I dispute this", or whatever wording you wanted put on there, because of a specific reason.

**Q62 Viscount Bledisloe:** I have to ask to see the report and then to put the comment on it?

**Mr Bradford:** Yes.

**Viscount Bledisloe:** I see.

**Q63 Lord Lyell of Markyate:** Experian's data, and you have got data on something like 460 million people, is supplied to a growing market in the use of personal information in a variety of businesses, no doubt very valuable. Can you describe the circumstances in which it is supplied in non-identifiable or aggregate form and those in which individuals remain identifiable? Do you try to influence your customers towards non-identifiability, where possible, in the interests of privacy protection?

**Mr Bradford:** My Lord Chairman, again with the example I have just given, I think, certainly for the majority of our business, it is based around the lender and a consumer looking at a very much consumer-based transaction. Clearly it is important in a case like that for the lender to be aware of that consumer's financial situation. The data may well be aggregated so that the lender gets a collective picture, but it will still relate to the individual. Examples where we would certainly not be looking to do that could be where we use aggregated and anonymised data at, say, postcode or postal sector level. An example of somebody perhaps looking to use that would be a major store looking to say, "Is this a catchment area with socio-economic groups A, B, C." So, we will do some geo-demographic profiling of that particular area, not using individual personal data, but using data that we have acquired from national census data, or whatever, that is in the public domain and that we can acquire. The difference between information that the consumer gives us for a credit application, which we certainly cannot use, and information which we can collect from within the general public domain, which we will then maybe model but you certainly cannot identify any individual, could be used, as I say, for store planning or something like that.

**Q64 Lord Smith of Clifton:** Could I follow that up? I would have thought that the ideal situation would be to take what is in the public domain about that postal code area and then read it across with the individuals you have in that area to see whether there is a mismatch or how far it equates?

**Mr Bradford:** It is an interesting point. I would love the answer to that question to be, yes. The reason we cannot is because the information that we hold at personal level is held for specific purposes; it is back to the fair obtaining clause. In other words, when I give my consumer data to Alliance and Leicester and it comes into Experian, I can only use that information for the reasons I agree to its use, and that will not potentially be for marketing purposes, it will not potentially be for putting with other data to form a view. The other thing as well: the UK shared credit information is governed by industry bodies, the British Bankers Association, the Council of Mortgage Lenders, which govern how data can be used, so Experian's credit bureau cannot unilaterally decide, "We have got these crown jewels and we are going to do something with it." It would obviously be good if we could, but we cannot, and that is both with privacy and commercial.

**Q65 Lord Morris of Aberavon:** If you have so much information stored, why, if I want to open a simple building society account, do I have physically to produce a fuel bill, a council tax bill repeatedly, time after time?

**Mr Bradford:** I cannot possibly comment on that particular building society.

**Q66 Lord Morris of Aberavon:** Every one. They say it is because of money laundering.

**Mr Bradford:** There are two things. This is a commercial answer, but I will give it nonetheless. We do provide online electronic systems that will enable that building society to comply with its money laundering regulation obligations. It is up to that organisation whether it chooses to do that. All I would say is that we have products that enable them to do it, but it is their call whether they use them. We have other organisations equally. I am sure if you walked into an Experian client to open a credit card, you would probably find that there would be online checks. I cannot speak for the individual lender, but clearly their own practices are such where they require paper proofs for that check.

**Q67 Lord Morris of Aberavon:** Take it from me, without exception, probably there have been half a dozen over the years that I have experienced.

**Mr Bradford:** You have obviously got a big commercial client opportunity.

**Lord Morris of Aberavon:** No. Nevertheless, the habit is the same.

**Q68 Baroness O’Cathain:** Is it not a feature particularly of a money laundering situation? Even if you have got an existing endowment policy, you still have to do it every two or three years and you have got to put in the same old thing when they know you very well and you have not touched the stuff. So it is money laundering, is it not?

**Mr Bradford:** It is money laundering, absolutely.

**Q69 Lord Morris of Aberavon:** I did say that. I qualified that when I asked my question.

**Mr Bradford:** Some organisations will still do that electronically.

**Q70 Lord Rowlands:** Is Experian interested in developing the market for more personal data for the public sector for either providing public services or for combating fraud in the public sector? If so, what implications are there for such developments?

**Mr Bradford:** My first observation would be perhaps sensitivity to the word “market”.

**Q71 Lord Rowlands:** You are a purveyor of personal data.

**Mr Bradford:** “Market” suggests a unilateral and bilateral use of information without the consumer’s agreement. I think we would be interested, we are interested, we are actively working with a number of government areas on how the public sector data and the private sector data can come together. As I say, because of commercial confidence I cannot talk about it here, but there are some significant government departments that we are in discussions with around potential products.

**Q72 Lord Rowlands:** That would be using data you have collected in the private sector in one way or another to assist a public service?

**Mr Bradford:** Yes, where we are allowed by regulation to use that data for the public sector, we will look to it to---

**Q73 Lord Rowlands:** Can you illustrate that first, because you have been making a very clear distinction all the way through your evidence that these are Chinese walls and there is information you must not transfer?

**Mr Bradford:** Yes, there is. There are two things that we cannot do with certain information. One we must do. One is to comply with whatever data protection obligation we have around that piece of data. If that piece of data were given to us on the back of credit risk assessments, we cannot then subsequently use it for something that is not a credit risk assessment with a public sector organisation unless that public sector organisation has a statutory right to access the information. For example, the Child Support Agency in its 1992 regulations actually lists the Credit Reference Agency as an organisation to which it has a statutory right to obtain data; so in that case we have to do it. In other cases, because the data Experian holds is obtained from commercial organisations, we can only use that data in line with what those commercial organisations allow us or licence us to do, if you like.

**Q74 Lord Rowlands:** I am not clear at all yet what sort of kind of data you can transfer to the public sector? Can you give an example?

**Mr Bradford:** There are two types of information Experian will hold, public information from electoral registers, to bankruptcies, to county court judgments to IVAs. There is data we will get from our commercial clients, which will be how somebody has performed on their credit card, dates of birth potentially. So, some data is our proprietary data, other data is data

that we almost hold on licence, and it is the data we hold on licence that we have to be very careful how we use in other sectors.

**Q75 Lord Rowlands:** Do you think that the relationship between the private sector and the public sector handling people's data, the kind you are now describing, generates a new regulatory problem of any kind or raises issues of the question of the role of the Information Commissioner, et cetera?

**Mr Bradford:** I do not think it raises regulatory issues. I think possibly what it does lay itself open to is a more positive private/public sector discussion and dialogue around how data can be used in two respective areas. When you think about a lot of the commercial organisations out there, to take fraud as an example, fraud is not confined to the private sector; fraud is in the public sector as well, as I am sure you all well know, and the same people are liable to be the "won't pays". I think in legitimate public interest areas like that, there is a lot that the two sectors could work on together. I do not think it is a regulatory issue, I think it is an opportunity.

**Q76 Lord Rowlands:** The systems are always enough to ensure the citizens does not get rolled over on it?

**Mr Bradford:** That is what I guess we have been talking about. Famous last words, I would have confidence in my private sector system doing that, but equally, looking at the transfer of possible data from private to public, we have to have that equal confidence that the things we have talked about, about knowledge of IT and so on, are as robust in the public sector. That is maybe where things come together.

**Chairman:** Mr Stevens, Mr Bradford and Mr Virgo, can I thank you very much on behalf of the Committee for joining us this morning and for the evidence you have given. The Committee will now go into private session to deliberate.