HOUSE OF COMMONS

Science and Technology Committee

Oral evidence: The big data dilemma, HC 468

Tuesday 17 November 2015

Ordered by the House of Commons to be published on 17 November 2015.

Written evidence from witnesses:

- Direct Marketing Association
- Nuffield Council on Bioethics
- Big Brother Watch
- Information Commissioner's Office

Watch the meeting

Members present: Nicola Blackwood (Chair); Victoria Borwick; Stella Creasy; Jim Dowd; Chris Green; Dr Tania Mathias; Carol Monaghan; Derek Thomas; Valerie Vaz; Matt Warman

Questions 98-186

Witnesses: **Chris Combemale**, Chief Executive Officer, Direct Marketing Association, **Professor Jonathan Montgomery**, Chair, Nuffield Council on Bioethics, and **Renate Samson**, Chief Executive, Big Brother Watch, gave evidence.

Chair: Can I welcome the panel to our session on big data? We are in the middle of an inquiry to understand the balance between the benefits and risks of big data. As you can hear, I have been struck down by a lurgy, so I will hand over to my outstanding Committee to ask the majority of the questions, but I am very grateful to you for making the time to come here today.

Q98 Matt Warman: You can hear me, hopefully, but I know Nicola will chip in at some point. Big data has been in the news hugely, and the volume of data being created has been growing exponentially. As the volume of data grows we hear a lot about the increased opportunities. Does that mean the risk is growing exponentially as well?

> ***Chris Combemale***: We all know that the benefits to customers, businesses and Governments of the big data era are huge in terms of efficiency, productivity and access to information, new products and services, but the pace of change is very rapid and risks are posed in terms of data security and having systems that keep up to date and up to speed and have adequate capacity. We know that there are hackers and criminals attempting to access the data, so it is incumbent upon businesses and Government to put the utmost

effort into data security, openness and transparency. Of course, there is great risk to people's brands and brand reputations, because in this era of big data honesty and trust are the currency of companies to do business with their customers. If you breach that trust either by using data inappropriately or by having data security breaches, the backlash is quite considerable and quick, because customers themselves have access to information and technology, and can act quickly through social media to name and shame companies they believe have acted inappropriately.

Q99 Matt Warman: Has the balance shifted? Is there a sense that, while the benefits are increasing, the risks are increasing at a greater rate?

Chris Combemale: I am not sure they are necessarily increasing at a greater rate. I think people are becoming more aware of them. In their personal lives, parents are becoming more aware of the risks their children might face and providing guidance on how to do it. Companies, and I think boards of directors, are becoming more aware of the risks. It is not that they did not exist before, but often, with regard to data, data compliance issues and data practitioner issues, boards left it to the marketing department or the boffins. If the way you use data and keep it secure is fundamental to the future of your brand, it needs to be a board level issue and chief executives need to be responsible for putting in place the right culture across their companies. That was why a year ago we changed our DMA code to one based on five principles that could act as a road map for putting the right culture into an organisation, which I think is more important than the details of the rules that compliance officers might look at.

Professor Montgomery: When the Nuffield Council was producing its report on biomedical data, we looked at what evidence of harm we could find. The main learning from that, apart from the fact it was very hard to find out as much as we hoped, was that it remains the case that most of the breaches are human as opposed to technological. That suggests that you would not expect an exponential change in the risks, and some of the techniques we have used previously to safeguard privacy and confidentiality remain important in terms of personal integrity and the quality of staff. There are, however, a number of ways in which previous safeguards are probably less effective. A particular one we identified is the ability to link together multiple datasets, so something that might not be identifiable in the hands of the original producer becomes identifiable when linked with publicly available information. The idea that it is relatively straightforward to anonymise data is no longer the case in the new world.

Q100 Matt Warman: We will come on to anonymisation specifically, but do you think that overall we are getting better or worse when it comes to data protection?

Professor Montgomery: I do not think we have enough evidence to suggest one way or the other. It has always been the case that health records have been accessible, due to human weakness, for people who try hard enough to do it. I do not think we see clear evidence of increased numbers of data breaches, although some of them are bigger in scale because of the way in which data are now stored. If you have one data breach, it releases more data than it has previously.

Renate Samson: This is enormously broad. Both Chris and Jonathan have touched upon a broad range of points. I do not think it is a case of better or worse or bigger or smaller; we have just become much more aware. As citizens or consumers we now understand much more clearly that every time we engage online or with a connected piece of technology we are providing data. As to whether or not that data is safe, there are still a number of question marks. The consumer and citizen still need to continue to learn. We need better engagement with any organisation, whether it is business or Government, as to what is happening to our data and what protections are in place. Equally, we need to understand what we should or should not be doing, and what we are comfortable doing with a piece of connected technology when we hand over anything that is personally identifiable about ourselves.

Q101 Matt Warman: Could you describe a little what is qualitatively different about big data, as opposed to the traditional areas where organisations like Big Brother Watch have campaigned to protect individual privacy?

Renate Samson: I am not entirely sure I understand the question.

Q102 Matt Warman: The nature of big data is different from the traditional areas that Big Brother Watch has focused on; it is about a surveillance state, which is a term you have used before. What does that mean when it comes to the large datasets we are now looking at?

Renate Samson: As Jonathan expressed, cross-referencing data between datasets could potentially be perceived as a form of surveillance, depending on who is doing it. When Big Brother Watch was originally established we concentrated a great deal on CCTV cameras. Technology has advanced in the six years Big Brother Watch has been going, and aspects regarding privacy and civil liberties are broadening. We do not live in a world where CCTV cameras are the only thing watching us. The mobile telephones in our pockets watch us; our Fitbits watch us. We are rapidly moving into a completely connected society with the internet of things. Therefore, the risks to an individual's privacy and security, bearing in mind they are two sides of the same coin, are now a concern away from just CCTV cameras and chips in bins, which are still equally a problem.

Q103 Matt Warman: Mr Combemale, maybe you can give us a sense from the DMA's perspective of how big brands use that, or take advantage of what if it was a state would be called surveillance, but you would probably find another word for it.

Chris Combemale: Perhaps I could answer in two parts. The first is to give an example of how a large dataset has been used in a very effective campaign. All of you might have seen the British Airways billboard campaign where a little boy points to an aeroplane as it goes by. It identifies the flight passing overhead, its destination and where it comes from. That uses two parts of data that have never been used in a marketing campaign before. One is operational data directly from the flight deck beaming down and being picked up by the billboard sites, but it also uses weather information. If it is cloudy where the billboard is located, the ad does not run with the boy pointing his finger, because the audience cannot see the aeroplane and it does not have an effect. You are using big data

for live streaming of real-time weather information, combined with flight deck information, to transform a billboard environment.

What is also important is the perspective of customers—how they view it. Every three years we run a study called customer attitudes to privacy. When we ran it earlier this year we saw significant statistical changes in several areas. First, there was a large increase in the number of people who agreed that sharing data was part of a modern economy. We have identified historically three sets of people—three distinct segmentations, if you will: data unconcerned, people who are not in the least bit worried; data pragmatists, who will share data when they trust a brand in a context they are comfortable with; and data fundamentalists, who are uncomfortable with the whole data economy and data sharing and who tended historically to skew older. This year we saw a reduction of 7%, from 31% to 24%, of fundamentalists, and the age break was eliminated, so the skew towards older people does not exist any more; and there was a huge increase in the number of unconcerned, up from 16% to 22%. As we move down the particular information age we live in, it seems that customers are getting more comfortable with what is happening. They are becoming more aware of the risk, but there is still a lot more to do.

Renate Samson: Equally, we did polling at the beginning of the year and found the absolute opposite. We found that 79% of people we made contact with were concerned about their online privacy; that 74% of them would like to control their own data; and only 25% of them did not mind adverts being tailored to them online. There was also, quite clearly, an element of confusion in people's minds. People accept that they have to give some data over to receive something in return, but their varying degrees of concern about that change according to who they are handing the data over to and a larger part of what we are probably going to end up discussing today is that it is not clearcut. You cannot say specifically, "I'm not happy to give my data for this," and that "this" means "everything". You want choice. You want to be able to make granular decisions. Currently, we live in a world where terms and conditions are, "Do you agree with this—yes or no?" As we move to a more connected society, yes or no simply cannot stand; we soon will not be able to have a yes or no choice as to whether we engage online. What we then need is, "Yes, we engage online because we have no choice. Now I want choice in every different aspect I engage with." It is important that we know what we are dealing with, that we are asked and that we are given respect and responsibility.

Chris Combemale: We would agree with that. Our study showed that 90% of people want more control, so while 72% were comfortable, they absolutely want more control; they want more openness and transparency, and they will work only with companies they trust, so that matches quite well.

Q104 Chair: Professor Montgomery, we have just had two contradictory surveys on public attitudes to data sharing. Do you have a third view?

Professor Montgomery: I cannot trade statistics, but we looked at some case studies as we were trying to understand people who come within the context of health data. One thing we identified was the relative acceptability of the Scottish system of sharing health information and the relative unacceptability of the care.data attempt in England. What we drew from that was that it was not so much to do with what was actually being done with the data, as with the trust and degree of participation people felt they had in shaping the

project and the understanding that it was something worth doing. In the care.data context, it was felt to be to some extent deceitful; it was thought to be a Trojan horse for selling data to commercial companies. It split the people who might have been advocating for it, so GPs in particular came out expressing anxieties about whether it was really an appropriate thing to do. That lost the focus of the argument about whether care.data as an initiative was a good idea and went into issues around trustworthiness and the competence of communication. That did not seem to appear in the Scottish context, although we do not know whether it would emerge were there some form of campaign against it or a scandal, but it is based much more on a tacit understanding that people feel the health and social care system is aiming to do something that benefits them and they have a stake in it. I do not know that it was ever particularly tested, so whether it would hold in the case of pressure we do not know. It is not about statistics; it demonstrates that the context in which initiatives emerge makes a major difference to their acceptability.

Q105 Jim Dowd: When I was on the Health Select Committee we looked at the ill-fated medical record scheme. We discovered that if people thought there was a personal benefit to them they were far more relaxed about sharing data. They were quite happy with that, but the technology did not work. Can we look at external threats to dataholders? We had the recent experience of TalkTalk and what went wrong there. A lot of people found it disturbing that those in charge of data for a considerable time did not know exactly how many records were involved, what kind of information had been extracted and so on. Is that going to be a growing event—I hesitate to say phenomenon—given both the scope, the width, of commercial activity on the net now and also the depth of the data records being held?

Chris Combemale: There is certainly a constant battle between data security and hackers or other malicious attempts, sometimes purely criminal and sometimes people with specific agendas. The same goes for foreign Governments sometimes trying to access Government data and policy. It is a constant battle. One thing I would say is that companies need to invest a greater amount in data security and in understanding that it affects their brand. TalkTalk has taken a hit as a result of that. They have particular challenges, on which I am not expert, in terms of legacy systems and legacy data, but every company should invest more than they are currently investing. Whatever the amount they are investing, they should increase it.

Q106 Jim Dowd: What was most disturbing about TalkTalk was that it was a communications company. You would have thought it would have a greater ability to deal with these things.

Professor Montgomery: I will not comment on TalkTalk. It is not just about focusing on data security issues; there is something about showing that you are competent and trustworthy by being open and transparent when things go wrong, and certainly in the context of public sector data making sure you push back to people the uses made of the data. You do not rely on them questioning; you make it accessible to them relatively easily. There has been talk in the health context of data statements about usage, to close the loop you described, in terms of people thinking there is something in it for them.

There is real cause for concern, particularly in the context of sensitive personal data, that breaches may occur and no one will say very much about it because nobody has a stake in

making it transparent. The company does not want to damage its brand and the person whose privacy has been intruded on does not want to admit whatever it is they feel embarrassed about. It is very important that we see some proactive steps. That is why we would recommend that this is not just a civil issue but a criminal law issue, because society has a stake in promoting the trustworthiness of the system. We have to assume there are more breaches than anyone brings to light, and that it is not just about front-line security. All parts of the system are vulnerable because of the human factors.

Renate Samson: My understanding is that last year 90% of all UK companies suffered some sort of attempt to hack into their systems. I am not technically able to give you a proper answer to the question you asked, but as the gathering of data increases companies have to do a number of the things that have just been mentioned, and there has to be an understanding inside the company. We now have to accept that, no matter what element of business you are in, you are in the IT business. Therefore, a lot of responsibility comes with that that maybe we are not yet touching on. Concern was aired on the back of that hack and other hacks about the encryption of data. For the economic wellbeing of the country and the security of all of us, it is important that we have a solid conversation about what data should be encrypted, pseudonymised and anonymised—all those different terms, which a lot of people do not understand.

Q107 Jim Dowd: We covered encryption last week when we were looking at the draft Investigatory Powers Bill. Since then I have read a piece about a client allegedly working for the FBI who hacked the Tor project, so there is clearly an arms race. In your estimation, what is the balance between those seeking to obtain data for gain—for commercial purposes—and those doing it simply for nihilistic reasons?

Renate Samson: I could not give you figures on that. We live in a society, and we have always lived in a society, where some people will do bad things for personal gain, or maybe just for the rush of it. Sometimes we can find ourselves in a place where we put the online world into a different sphere, but we have to accept that much of what happens in the online world is the same as happens in the analogue world. People behave badly in both areas. Just because we cannot see data does not mean that we should not protect it in the same way as we protect a physical ledger.

Q108 Derek Thomas: You mentioned the kind of consent which at the moment is basically yes or no, and in lots of cases that is all that is required. Has the Consumer Rights Act 2015 led to more informed consent for consumers? Are there other ways in which they should be asked for consent, and has the Act helped to inform consumers?

Renate Samson: I think it came into force on 1 October of this year, so I cannot give any answer as to that Act. I think it is a step in the right direction. It encourages people to be aware that they have rights when buying online products—an online book, for example. Yes, it is a good move. If anybody has an iPhone, the recent Apple update is granular. It is not perfect, but you are asked every step of the way after updating to iOS 9 whether you want to switch it on. You are asked, "Do you want to have location services on—yes or no?" rather than, "Yes, accept this update." You are asked, "Do you wish to turn on the cloud? If you turn on the cloud, which of these different aspects of your mobile telephone do you want to be on the cloud?" That is most definitely a start on the right path to give

consumers and citizens a choice as to what they want to engage in and what they do not, rather than, "Yes, it's all on," and your data are being shot out everywhere to all and sundry. I am now able to choose not to use iCloud and turn it off. If I do not want to have location services on, I will turn them off, but when I download an app and it says, "We would like to have access to your camera and microphone," I get to choose whether or not I want the app to have that. It does not need to have access to my microphone in my opinion. A communications app may, and I have to determine whether or not I am happy for them to do that. That is good. I now have choice, and I think that is important.

Chris Combemale: I would agree with that.

Professor Montgomery: We would be nervous about putting too much weight on that. We are entirely supportive of it, but it remains the case that the majority of people will not think much about those choices and will not read it through. Fortunately, when I read the terms and conditions, I did not download a rugby world cup app that would have shared my contacts book with the company. I could not see any reason why it would need to do that.

We have argued that, in addition to the consent-type process where you have the option to opt in or out of particular components, we also need to focus on transparency questions—how clear it is and the purposes for which your data are being collected or collated. We talk about it in the context of the public sector as being publicly stateable and morally reasonable. I guess that in a commercial context it would be mutually acceptable. You might do something which to other people would be morally strange but you know you are doing it, so it is bringing together the consent bit with how likely it is that people know that and how transparent the process is—the deal you are signing up to.

Chris Combemale: There is another opportunity. One of our main issues is to write consent statements and privacy policies in clear, simple, down-to-earth English. A marketer has a piece of real estate, which is the point at which a potential customer will decide to engage, and they allow the lawyers to write the language in a way that is indecipherable to anybody else, when you spend thousands of hours and pounds crafting every single word of the rest of your communication. It can be proven through A/B testing and multivariate testing that well-crafted permission statements in plain, simple English lead to a greater number of people registering and sharing, and that builds trust for the long term.

The other thing we do is to distinguish what we call good consent and bad consent. Good consent is when it is clear, simple, open English that makes the value proposition in the exchange particularly clear. Bad consent is when someone is tricked into consenting without realising it, because there is a pre-check tick box, or whatever the case might be. It is emerging clearly that a relationship you build with your customer based on good consent endures better and leads to more repeat purchases and brand loyalty. There is a commercial imperative in being clearer, more open, more transparent and more honest in what the proposition is, and that leads to a better, sustainable relationship.

Q109 Derek Thomas: It sounds like we are heading in the right direction, but for a consumer how practical is it when they cannot tell? It sounds to me that if I want this service or product I have to consent; I have no choice. It is great to know everything about it, but at

the end of the day, if I want to find my way to somewhere through a sat-nav, or even access a purchase, unless I consent to what they are asking I do not get the product. Do I just give in and consent?

Chris Combemale: There is increasing availability for people to compare products and options in the world. No one is obliging anybody to buy a particular product or service. If you are not comfortable with the proposition—the privacy statement and the consent is part of the product proposition in today's world—and you are not happy with it, you should seek an alternative provider of a similar product or service. That is a click of the mouse away with Google Search and whatever. The consumer has access to greater ability to comparison shop and compare propositions than ever before. It is up to the customer to make that decision. If they are uncomfortable, they absolutely should not do business with that company. There will be another company who are building their proposition on openness, transparency and long-term brand loyalty with whom they should consider doing business.

Renate Samson: I wholly support that. It comes back to what I said. With the Apple device in the instance I gave, you have choice as to what aspects of it you want to use and what you do not. It is no longer the case that if you have the device you now have to do everything they tell you to do. When you are choosing an app, as Chris said, if you think one app is offering you something you are nervous about, you do not have to have it—you really don't; there will be enough others on the market. Even Google: if you do not like Google, you can use DuckDuckGo which does not store or retain any of the information about your search. You are not obliged to use only Google, or only one type of map, be it Apple or something else. There are now choices, and that is important. The fact that we are even having this conversation is a huge step in the right direction.

Q110 Derek Thomas: It is about giving power to the consumer and letting them know they have it.

Chris Combemale: And they do. The consumer has never had more power than they have today in being able to investigate companies, compare manufacturing abilities and compare their approaches to ethical manufacturing standards, and find out where people are shopping. As long as they use that ability, they can comparison shop. Brands have to make the approach to privacy and the building of trust a central component of brand value and brand equity. Those brands that do, and make it central to their proposition, will gain more customers over time than those that do not. In the end, you cannot trick or lie your way into a long-term business relationship.

Renate Samson: You have a slight problem when you sign off terms and conditions. You sign off and say, "Okay, I agree to this," but terms and conditions change, and we are not always informed clearly that they have changed. Over the course of the last few months Uber, Spotify and Snapchat have changed their terms and conditions. Snapchat is meant to be about private photograph sharing, but it now says, "We can make your private photo public if we choose." Uber has now made it quite clear that it will store personal information about you specific to your location. I appreciate that is a benefit to its service, but you may become a loyal brand user and then the terms and conditions change. You are wrenched away from a service you have come to rely on and you then have a possibly difficult choice to make. People who use Spotify got very upset about the fact that it was

suddenly going to access photos and contacts. It claimed that it was tailoring your user experience. It is my experience; I am the user. Please do not make an assumption that because I want to listen to some music you need to determine what music I need to listen to based on my photos.

Q111 Chair: I want to go a little further with this. Mr Combemale, when you opened you gave the example of two datasets—weather and flight data—being used for advertising. Those two datasets were not gathered for that purpose. The whole point about big data and its potential is the use of datasets that have been gathered for another purpose being put together to produce a different outcome. How does consent fit into that? People might have consented to the initial data gathering, but it is consent to the second step that is the challenge, surely.

Chris Combemale: Weather data are interesting. IBM just bought the weather company that is one of the collectors and providers of weather data, but that is open and available. I do not think weather data relate specifically to individuals. Maybe a better and more relevant example is what happens in loyalty programmes, like Tesco Clubcard, Nectar and the new Marks & Spencer Sparks programme, which have transformed the type of discounts people have available to them. In the past, you got coupons and other discounts on a random range of products, many of which you might never have bought, and never intended to buy. Today, you get discount offers on things you have purchased in that company before and are likely to buy again, so you accrue the benefit and, hopefully, in their mind stay brand loyal. Sparks, Marks & Spencer's new loyalty programme, has gone one step further. They allow you to select from a range of potential discounts, say 20% on clothes for the next month. For the next month, any time you buy those things you will get the discount. To go back to what Big Brother Watch was saying, they are shifting more control to the consumer to give them the opportunity to select their benefits. They are also allowing them to select charities to which to donate on each purchase. That is an example of how things are shifting from completely random offers to tailored offers, and giving control to customers. I think that is beneficial.

Q112 Chair: I am not sure that quite answers my question.

Professor Montgomery: There is a major legacy issue. I find it very difficult to opt out of direct marketing calls at home, because I can never get transferred to anybody who will take me off their database. I am told that if only I answer their questions they will not ring me back, but I'm afraid I don't believe them. There is something about balancing the good practice that is now emerging with the legacy challenge. That is one of the reasons why we feel that consent is a difficult concept to put too much weight on, because of the repurposing, the change of conditions to which you initially consented and the transformations of ownership. You probably did not think about what has now become possible with new technologies at the point you consented. While we need consent and transparency, we do not believe that consent is sufficient. We need to build with that transparency obligations to give an account of why you do things. We also need governance processes in place to reassure people that, whether or not they exercise those controls, the terms on which the information is being used are being honoured by the organisations. I guess you would say that is part of the trustworthiness offer.

Renate Samson: In relation to the question you asked, that feels like third-party data sharing. I have booked a seat on a plane and now you will know that I use Virgin Airways—my data knowledge or whatever. I am moving away from it slightly, but the point is that I feel nervous that companies are sharing data to benefit themselves by telling me what the weather is, even though I may receive a benefit in knowing that, but I can find out what the weather is regardless of them having my data. If there was an ideal way of doing this, I would like to see in the terms and conditions the list of third-party organisations that my data will be shared with by that organisation. I know that will be long-winded and I appreciate that many companies will say, "Today, I know that I want to share your data with these five companies, but tomorrow I might suddenly find a benefit in sharing it with five more. Do you really want me to email you and tell you?" to which my answer is, "Yes, I do. I want to know who you are going to share my data with throughout, so I can say whether or not I am happy." That is explicit informed consent.

Q113 Chair: You favour explicit consent. Professor Montgomery, is that also what you favour? This is what is being discussed in the EU directive.

Professor Montgomery: In the health and biological context, explicit consent is problematic for a whole load of things we have come to rely on. It is already the case that we find it more difficult to set up disease registries, for example, than we did previously. It is widely anticipated in the health communities—I am not speaking for Nuffield at this point—that the new data regulation will create difficulties, because of the problems of going back and asking people who were quite happy with the ground rules initially. They cannot easily be found now because those data have not been held. That is a different sort of context from the one we are talking about. The proposal we would make is that you can address that through more participatory governance processes for working with the communities, which will give you a much better understanding of what people are and are not anxious about.

There are significant questions about whether specific consent will give us better protections, because of the problems of knowing whether people understand the information and the legacy challenges of historic consent. It may put barriers in place in terms of things that people think are quite important but do not have a mechanism that they can easily engage with. I think we have to have the chance to debate those things. The idea that you have done the job by getting a consent is a little too seductive. My background is as a lawyer. There is plenty of evidence that lawyers think the more you put in the form, the more you pass the risk to the consumer. I do not think it duly respects the interests of consumers to think that consent passes risk in that way. There are some traps about consent, as well as the fact that it is one of the very important mechanisms for respecting people's rights.

Renate Samson: There is a flipside to this. The way we go about it right now is not necessarily the only way we should go about it. There is an opportunity, in that I hold all my data and the company comes to ask me for what I want to hand over, rather than the current system where the company holds all my data and asks me which bit I agree to. There is another way of looking at it.

Q114 Carol Monaghan: I want to pick up something Chris and Renate mentioned about downloading apps. Of course, we can click to agree or refuse. That is probably fine for somebody who is technologically literate, but for people who are possibly more vulnerable or who struggle more, is there a danger that they just accept? Do we need to put protections in place for those people? I am thinking of elderly people. My father is an 80-year-old iPad user who will download and agree to anything. Do we need to have protections in place for such people?

Chris Combemale: The current Data Protection Act, which was enacted in Europe in 1995, and in 1998 in the UK, adopts eight fundamental principles, one of which is that data should be collected only in the amounts and types necessary to produce the services you are delivering. There is a fundamental notion that, if you are developing an app, you should not collect data that is not necessary for the delivery of that product or service. In that sense, people who within their apps are downloading your contacts are very much in breach of current legislation. Those protections exist. Earlier this year, we very much welcomed the fact that the Information Commissioner received additional fining powers of up to £500,000 in civil monetary penalties to enforce against people who are misusing data. A large amount of protection already exists, but the consumer may not be aware of all the protections they have.

Renate Samson: In answer to your question, yes, there is a need for the vulnerable in society to be better informed as to how to go about understanding terms and conditions. That applies to all of us, not just the vulnerable, but most definitely the elderly. My organisation now creates factsheets where we try to explain complex or simple issues, such as how to create a password, in a very straightforward, easy to understand and non-technical manner. An awful lot of charities and organisations are trying to engage people across all sections of society on how best to stay safe online, but more can definitely be done.

Q115 Carol Monaghan: Should there be some sort of responsibility on the app producer not to gather data where it is not required?

Renate Samson: Absolutely. As Chris said, that is in the Data Protection Act.

Chris Combemale: We publish a guide on vulnerable consumers, particularly training modules for contact centres to recognise when something might be appropriate. My mother in the US had this situation. She had Alzheimer's, and 40 copies of *Time* or *People* magazine would arrive. We cancelled them all and two months later they would come back again. It is an issue that I am personally passionate about. It is quite easy for a company to recognise when someone who may not have their full capacities any more is repeat purchasing products that have no need to be repeat purchased. Companies have to take their responsibilities to society correctly, and we need to help them understand how they can identify those cases.

Professor Montgomery: That is a reason why consent is not sufficient. It is important but not sufficient. Those things are consented, but you are not fulfilling your responsibilities by accepting the consent.

Chris Combemale: You end up in a strange place where the person is still legally competent to make unfortunate decisions and the family is not able to intercede, so it becomes incumbent on companies to act responsibly in how they go about their business. We all know that, while that is the majority of companies, there are rogue traders who do not particularly care and will prey on the elderly. That is where enforcement becomes important.

Q116 Victoria Borwick: Professor Montgomery, in your earlier submission you said that "neither consent nor de-identification is sufficient to protect individuals' interests." Do you want to come back to us a little on informed consent? You began to touch on it in your earlier answer.

Professor Montgomery: I probably covered most of the consent issues. What are the challenges around consent? The first is what you have consented to. We have explored the problems of things changing over time, what people understand and how well they understand it. The second is about what it does to responsibilities, and we have just touched on that. Do I accept responsibility for everything I have consented to? Even if I have read the terms and conditions and understand them, it might not be a fair offer to make; it might be inappropriate to exploit my consent to that. There is also a whole set of things about uncertainties, so the idea that you can have informed consent that covers all the things that might turn out to be relevant to the consumer is problematic. You need to think about informed consent as involving two separate things: the obligations to inform and the issues about getting the consent. We tend to elide them a little too easily. Those are the key things about why we should improve and promote consent processes, but we should not think that they do all the work that needs to be done. Is that a little clearer?

Q117 Victoria Borwick: I think so. Personally, I think it is a very good idea in respect of some of the topics you mentioned.

Professor Montgomery: We were not saying it is a bad idea, but it is not a sufficient idea to do all the work that needs to be done.

Q118 Victoria Borwick: I understand that. What do you think the Government should do to promote good practice on obtaining consent where it is needed?

Professor Montgomery: It is to do with the risks to which people are exposed when they give consent; if the risks are reasonably de-identified, and are reasonable trade-offs that benefit you and the value proposition is roughly comparing like with like—I give up a certain amount of freedom to get a certain gain. It is much more difficult where there are knock-on effects that you might not necessarily see as being connected. That is particularly where questions around repurposing linkage become important, because the person to whom you initially give the data may not be the person you become concerned about ultimately. In those contexts, we need a legislative framework that encourages the transparency of linkage projects, provides them with some obligation to demonstrate what they are doing publicly, therefore enabling a discussion about it, and has some sort of governance mechanism to hold them to those statements, but that also protects people's ability to pull out if it turns out that they agreed to something that has morphed into

something very different. I do not think you can rely just on the individual to deal with that, because the scale of things that happen to my data is well beyond what I will have the time to track. We need to look at processes that put those three pillars into place—a system that it would be worth trusting.

Q119 Victoria Borwick: Inevitably, as you said earlier, health data are slightly different. I very much liked the way you explained to us how you work through a sort of ladder in conceding or approving data. That depends on what happens to your health data and where it would end up, which might not be the same, particularly if it is anonymised, and then you do not have that option.

Professor Montgomery: We need to be aware that what counts as health data might not be quite what you expect. My credit card—Sainsbury's record of my buying alcohol—will be as good an indicator of my health as my GP records. I do not go to my GP very often but I quite often go to Sainsbury's and buy bottles of wine.

Renate Samson: I have to interject briefly. That is one of the problems we now have with algorithms and assumptions in datasets. When I go to the supermarket and buy 15 bottles of wine and four packs of beer and put them in my fridge that is connected online, that fridge, the insurance company and the healthcare organisation may assume that all of that is for my personal consumption. I am teetotal, but I host a book club once a week. I provide that alcohol for my friends who are coming to visit. I am then going to be punished, or there will be an assumption that I have a drink problem, or that I eat too much cheese, or whatever else might be in my fridge. Without my sitting here having this conversation all of you might believe that.

Victoria Borwick: You should see my supplies of chocolate.

Renate Samson: Exactly. We have to be very careful that we are not making assumptions based on datasets. It is inevitable; these things happen. We make assumptions all the time in life, but when it is not an individual turning round to another individual asking the question but assuming something is the case we are on the very slippery slope of not trusting people, punishing people financially and restricting their access to basic services, or to a home or proper healthcare. I am very nervous that I am not in the position, as was pointed out, to be able to track all the data about me that are out there.

Chair: You are talking to a chairman who received an email this week offering to plan my funeral. I do not know where that came from. Maybe they heard my voice.

Q120 Stella Creasy: The Consumer Rights Act did not give consumers any new powers at all. On some of the questions about data, forward motion has been driven by commercial interests rather than citizen interests. One of the best examples is midata. The midata project has stalled because it is led primarily on a voluntary basis by the companies. Obviously, if you are a company you do not want to share the data of your consumers in a way that is meaningful, because you might lose customers as a result. In the first evidence session in this inquiry Dame Fiona Caldicott made what I thought was an extraordinary statement; she said that your medical records are not owned by you as a patient but by the Secretary of State. Where do you think we can learn, in terms of bringing a citizen perspective to how data are

managed especially on things like midata, about ownership of data? I noted that earlier, Renate, you talked about owning your own data. What difference do you think that would make in the commercial sector, for example in projects like midata, and in the public sector where we can learn from, say, the Swiss health bank example? Perhaps we could start with you, Chris, on midata and where it went wrong.

Chris Combemale: The benefits have to be easy to access and easy to gain. I was looking at some of the things you have to do, or the communication from banks about midata, and the utility companies and so on. It seemed like too much hard work for the benefit I might gain from marginal improvements in interest rates and so on. To me, even as a consumer, not just as a representative of an industry, the whole issue of comparison shopping in the utility space is shrouded in mystery. It is unclear to me how I figure out exactly what price I am paying and what I am going to get. In some of the examples where it has been applied the potential benefit might not have justified the amount of work that was necessary, and it may be too difficult for the consumer to make the direct comparison.

Q121 Stella Creasy: What is quite clear is that for the companies there is no benefit in collaborating on a consistent portable form of data, because in the banking industry where that has been imposed there has been a lot of switching. They have lost customers. What I am asking is where, perhaps from the consumer perspective, we could change things so that the benefit of owning our own data would accrue; for example, being able to say, "This is the data I want," so that I can compare my energy bills or my banking costs, because they are in a data format that makes sense to me.

Chris Combemale: I think it is a fine balance. In the research we did, 82% of customers believed that the data belonged to them. That is right; their personal data is theirs. Their shopping patterns and shopping habits accrue to them.

Q122 Stella Creasy: But I cannot go to Tesco and ask them to give me my Clubcard data in any meaningful format so that I can then go to Sainsbury's and compare like for like.

Chris Combemale: No, but one assumes that people know what their shopping is and what they buy. As Renate just demonstrated, she knows she buys four bottles of wine and the purpose for which she buys it. Only the consumer can know that. Tesco can never know the purpose for which she made those purchases.

Q123 Stella Creasy: The point of midata was to be able to give consumers portable data so that we could compare. We could use big data for ourselves and compare the costs of our energy bills and financial services and perhaps the cost of our weekly shop against other companies in a fair and transparent way, and choose to apply our custom accordingly.

Chris Combemale: Some of that is happening in the supermarket base, to which we have already referred. I happen to go to Sainsbury's. Every time I shop I get a little printout that says that my shop was more or less expensive. I have never validated or verified that, and I do not know how they know all the competitors' price points.

Q124 Stella Creasy: With midata that was very specific. I could compare, for example, a current account at one bank with a current account at another in a meaningful and portable way in terms of my use of banking. Why do you think that has not worked in the energy or insurance sector, for example?

Chris Combemale: I am not particularly expert on midata in the energy sector, because we cover all sectors rather than a specific one, but I suspect it would have to do with the ease of use, awareness that it is possible and various other things.

Q125 Stella Creasy: Do you think there is any commercial imperative to making it harder for consumers to access their own data?

Chris Combemale: I do not think there is a commercial imperative for making it hard, but if a company has invested time in getting to know you, just as you might invest time in getting to know a friend, the benefit of investing that time, trialling different offers and finding out things is some of the proprietary or commercial knowledge you have built up that your competitor has not. At the same time, I fully understand that someone's shopping history belongs to them, but at what point does a company, who may have spent 20 years servicing your needs and becoming very close to you, give up all that information to their competitor who has not invested that time and effort in getting to know you?

Q126 Stella Creasy: When they offer me a better deal would be the answer. Professor Montgomery, it is the same thing in terms of healthcare, isn't it? Would direct explicit ownership of data by patients change some of these debates?

Professor Montgomery: It is tricky. Ownership is a very tricky concept to use for a number of reasons. The first is that this is not data that pre-exists; it is produced when you go into the system, so in your health records are things about you. There are things that you put in and there are also assessments and judgments made by doctors and others. It is more co-owned than owned by one person rather than another. If you make it portable, you are also taking something of the doctor's judgments into that. Part of the resistance has always been because of that element of co-production and the stake that doctors have in it. Rather like Renate, I have long thought it would be very nice to make the health record system something that is controlled by the patient and which providers ask to plug into; they get permission to use it for certain purposes, but it is controlled by the patient. But to do that I would have to have the ability to control the judgments of my GP and surgeon as they make sense of what they see. It is complicated, but what it does expose—

Q127 Stella Creasy: The example of the Swiss health bank is that. Could you contrast that with what we do here?

Professor Montgomery: The bits of work going on that I am aware of that we would need to do better before we could make it work here are, first, systems quality and the ability to transfer things, which, as I understand it, is quite similar to the midata concept. There are also major problems of data quality. The further away the interpretation of the health data gets from the person who produced it, the more scope there is for it being misinterpreted. There is work going on to try to improve standardisation and the way we record things,

which would make it more possible to translate those things. None of those stop it being sensible to think that I should take more control over my own records, because I am in as good a place to interpret them as the GP because I have co-contributed to them, but I need some interpretation. Extracting them as if they can be understood without reference to context is problematic in health data, because people record things in so many different ways. It needs more work.

Q128 Stella Creasy: The Swiss bank asks you every single time somebody wants to access your data for a research project. It answers the question about third-party access, doesn't it, in the public sector?

Professor Montgomery: It enhances my control and I would be supportive of that. It does not necessarily improve the quality of use to which the data is put, because I might release it to someone who then misinterprets it and it becomes inaccurate. I could be harmed by the inaccuracy, and I might not be in a position to tell. The simplest thing is acronyms, which vary from hospital to hospital. If you take an acronym from one place and interpret it as meaning something different, you could make a misjudgment, which is why most of the projects on trying to integrate health records have ended up with quite narrow datasets around drugs prescribed, allergies and things like that because there is less scope for variation.

Q129 Stella Creasy: Renate, I presume you take a very different perspective on the idea of what it would mean in terms of projects like midata and healthcare projects if patients and consumers directly owned their own data.

Renate Samson: The word "ownership" is complex. I am not sure it is the right word, although I find myself saying it all the time. We are living in a world where so much change has happened so quickly that most of us have adopted the changes as we go along. It feels like we are on a path where we have to stick with what has already been predetermined. I do not think that is the case. We have lived in a world of change; we do not have to follow this path. We can turn it around. We can turn it upside down and give the individual citizen more control over their data without it being as disruptive as I think many of us fear, or having a broader sense of nervousness about it.

My understanding with regard to medical records—please correct me if I am wrong—is that prior to them being digitised you could pay £10 and get them. Parts would be redacted, which I presume would be comments the doctor had made about my frame of mind when I turned up with a broken leg or whatever. Let's not forget that just because it is digital does not mean that real-world value should not apply to the data we are sharing and using. We cannot just say no; we have to look at other options.

I do not think midata has failed or not been adopted. It may not have been in the form of midata, but I hear regularly in conversations in panels a number of proposals to try to create control for the citizen and the individual. I think we are on the precipice in a good way, not a jumping off the cliff way but a flying way. As there are more and more data and greater connectivity happens, people will be calling for that. When I go to Tesco they do not just have to take my data and that is the end of it. We can have an engagement where they say, "You now have a passcode and you can log in and see everything you

have bought today. You can store it on your machine and make a choice as to whether you want to come back and have a relationship."

Q130 Stella Creasy: Do you think we should take a lesson from Australia where they have gone one stage further and allowed third-party access to personal data? As a consumer I could say, "I'm going to give Sainsbury's all of my Tesco data," and they can come back to me and make me a better offer for the shopping I might do this week as a result, on the basis that I and several other people in my road are all going to buy milk on the same day.

Renate Samson: I genuinely do not want to speculate on that.

Q131 Stella Creasy: The flipside of this is where you give the consumer powers.

Renate Samson: That is absolutely right. If a consumer—not me—wanted to do that, it is for them to have that conversation. I would rather I said, "I want to share it with Sainsbury's," than that Tesco shared it with Sainsbury's without me knowing.

Q132 Carol Monaghan: Renate, you were talking about the ability to tie up sets of data. I suppose there is a worry that anonymised data, if it is not 100% secure, can be hacked into. Big Brother Watch has said: "Taking an anonymised dataset and linking it with another anonymised or open dataset can lead to individuals or groups of individuals being re-identified with relative ease." There is some concern around that. How realistic, therefore, is it that data can be anonymised to an extent that it prevents individuals being re-identified if different datasets are combined?

Renate Samson: I hold my hand up and say that I get confused by the different terms—anonymisation, pseudonymisation, hashing, scrambling; all those different words are used, often incorrectly. I do not want to get into that for fear of doing it. However, a number of studies have been done by people far cleverer than me. Anonymised data does not usually mean that you cannot reopen the data. For example, there has recently been a study by either Harvard or MIT which discovered that four pieces of information relating to purchases made on a credit card can be put back together so that 90% of people can be re-identified. *[Interruption.]* Are you recording this conversation? With just two pieces of information, essentially, anonymous information about purchase details—numbers from the purchase—40% of people can be re-identified.

There has also been a study regarding South Korean registration numbers, which are similar to our NHS numbers. That was pseudonymised information, in that part of it was completely hidden and the bit that was exposed was encrypted—it was scrambled. I can send you more information about this afterwards if I am slightly off. Using two different studies, the researchers were able to re-identify in both cases 100% of the individuals. That was with a 13-digit number. Our NHS numbers have 10 digits, but how they work out the codes which are specific to your geo-location is the same principle. In our submission to the Committee we gave two other examples where people had been re-identified based on what was perceived to be anonymous data.

Professor Montgomery: In the context of health data, the difficulty is magnified by the fact that in order to be useful the data has to be quite rich about your health. The richer it is, the more possible it becomes to use those techniques to correlate. There have been a few studies about the ability to identify the conditions Senators in the US suffer from by comparing publicly available data on tax records with data made available by health insurers, but on a wholly anonymised basis—they thought. Rather than thinking that it is possible to protect people's interests by asking them to anonymise things, we have to ask how we build in protections so that, even if that anonymity is broken in some way, sanctions still attach to that and there is comeback.

Q133 Carol Monaghan: That leads to my next question. Is it the case that data managers have to be better educated about how to anonymise, or maybe take it a step further and protect the data they are in charge of?

Professor Montgomery: We would say yes, but we do not think that would be sufficient. We feel there is a need for a criminal sanction. If it is in the hands of someone who abuses private information, whether or not you can track through the chain by which it came into their hands, there should be stronger sanctions than the civil ones, principally because no one may want to make too much fuss about the breach. There needs to be the ability to step in and say there is a broader public interest in making wrongs actionable.

Q134 Carol Monaghan: Is there a feeling that data managers are sometimes deliberately ignorant of such things or that it is too big a burden on them to try to keep data securely?

Professor Montgomery: From the data we had, which was quite focused on health issues, it was more mistakes and incompetence than deliberate, but I do not know what the data is elsewhere.

Renate Samson: I am not aware of deliberate breaches being a common thing. More often than not, it is a mistake or an error. We also have to accept that as soon as any piece of information is digitised it becomes immediately vulnerable.

Chris Combemale: There is a definite shortage of properly trained data scientists coming into the economy today for the amount of requirements that exist. I know that within the curriculum coding has become reinstated, but we believe that while people are learning coding they should also be learning about their responsibilities with regard to the use of data, not just for their own personal protection as citizens, but so that if they go on to take jobs in this area they have from an early age an understanding of the necessary balance and they learn the techniques of security and anonymisation as they go through the education system, if they think they might choose such a career. A career as a data scientist is parallel and related to a career as a coder or a developer. We would certainly like to see more done around that aspect of the curriculum as it goes forward, but I know it is not easy negotiating curricula.

Q135 Carol Monaghan: You have a DMA DataSeal kitemark. How much protection will that offer people against re-identification?

Chris Combemale: DataSeal itself is not designed to protect against that. It was a standard we created for companies that do not have an ISO standard on data security and data transfer. It looks at processes within companies as they go about their daily business—some of the things Jonathan talked about earlier, where within a business process people might download files to laptops and share them with colleagues, and they may not be encrypted or password protected. What we are doing with DataSeal is trying to create a minimum standard of awareness in companies that may not be heavy users of data, in the sense of medical records, to sensitise them to their obligations, and put processes in place that ensure minimum standards of data security and data knowledge within every company. It is not specifically designed to address the issues we have just been discussing.

Q136 Carol Monaghan: It would not necessarily protect against re-identification.

Chris Combemale: It would not get involved in any way in anonymisation, re-identification and things like that. It tends to be more fundamental basic hygiene processes where, as I think Jonathan said earlier, there is considerable scope for unintended poor practice to exist. It is as simple as people leaving a laptop on a train that happens to have a downloaded Excel spreadsheet on it that contains customer information—things we think happen quite regularly. In normal day-to-day business, apart from all the work around big data we have discussed, there is a need for greater knowledge and awareness and better processes in probably every company, large and small.

Q137 Chris Green: I want to turn to crime and punishment. This is mostly to Big Brother Watch. There are criminal penalties for hacking data. Is there a case for introducing criminal rather than the existing civil penalties for breaches of the Data Protection Act?

Renate Samson: Section 55 of the Data Protection Act, as we have heard repeatedly, does not give any opportunity for there to be a custodial sentence if there is a breach of data. The ICO can impose just a financial penalty. There is, however, a facility embedded in section 77 of the Criminal Justice Act. That is a dormant piece of legislation. Were it to be enacted, the opportunity for custodial sentences could occur. We are supportive of that. We think that it would be a very good deterrent to make sure you handle data correctly, but we would want it used in only the most serious cases.

A report we put together earlier this year showed that in local authorities there are on average just under 2,500 data breaches a year, but we found that a lot of it was people incorrectly sending emails, losing laptops or losing USB sticks. In one instance individuals were using CCTV to watch a friend's wedding, which is inappropriate and should be dealt with accordingly. We would say that as yet there are not proper penalties for misuse of data. As data grows, data-gathering grows and more data occurs, there needs to be a deterrent and an awareness that you cannot just mess around with this stuff.

Q138 Chris Green: As more and more data accumulates and is used and manipulated in more and more different forms, there is a greater case for criminal penalties, but doesn't current legislation already cover most of those areas: for example, unauthorised access to computer materials under the Computer Misuse Act 1990? Aren't these things already covered?

Renate Samson: Yes, there are areas, but the fact is that there is a piece of dormant legislation. Legislation exists to do this but it has not been enacted. It is not just Big Brother Watch that has called for that; the ICO, the Home Affairs Select Committee and the Joint Committee that looked at the Communications Data Bill have called for it. There is a broad call for section 77 to be enacted. In the European regulations being discussed currently the penalties will be much more serious than they are right now. The Information Commissioner will have much more opportunity to impose proper fines and penalties. Equally, I am aware that section 8 of the draft Investigatory Powers Bill has provision for the unlawful use of data, which potentially would lead to a spell in prison.

Q139 Chris Green: Mr Combemale, would there be a bit of concern in commerce if we started giving people a criminal record for accidental misuse of data?

Chris Combemale: Certainly for the accidental misuse of data, but there is a set of rogue traders out there who wilfully misuse data. There are criminal enterprises that wilfully misuse data and prey on the elderly and vulnerable. We have consistently supported calls for greater enforcement powers for the ICO to put those illegitimate and rogue traders out of business so that legitimate business can develop a healthy relationship of trust with customers. That still leaves some issues of lack of awareness, where companies, with the best of intentions, get it wrong. I think we can deal with that.

We consistently called for the powers that recently increased fining capability to £500,000. Adjudications in some recent cases have had quite high civil monetary penalties. We would support the Information Commissioner in his call for that dormant legislation, but only in instances of serious rogue traders, persistent offenders and genuinely criminal enterprises, not for unintended or accidental behaviours by companies and employees who are trying their best to get the balance right.

Professor Montgomery: I would concur with the position that has been taken. I have said a little already.

Q140 Valerie Vaz: We touched on the EU. It took a court case before we got the right to be forgotten and delete our history. The EU is looking at new regulations, and some of the highlights are the right to be forgotten and that consent should be explicit. All those enactments will hopefully be put in train. What is your view about them? Do you think they go far enough, or do they go too far?

Professor Montgomery: I have already alluded to the concern of people in the health community that there are projects that rely on the integration of data and which people would like to see happen because it would give them more responsive and effective health services. We need to bear in mind how much of the healthcare we give is not properly validated—we do not know as much as we should about it—and how much of the evidence we have to support healthcare is based on trials in somewhat artificial contexts. One of the promises of big data and the integration of health records is that we might learn what happens in the real world when people are offered particular treatments or drugs. There is some concern that we need a proper debate about the gains as well as the risks involved. There is certainly a perception that the weight on specific consent as the key tool might remove a lot of opportunities that people would like a chance to talk about. If we

could find a way of controlling that better, there might be things that would be ruled out by too great a compliance tick-box approach. There is a series of concerns which I am sure will be represented to you by other witnesses.

Q141 Valerie Vaz: Is that specifically about the EU regulations?

Professor Montgomery: There is a very significant concern about the impact it has on health data registries of various sorts, particularly in relation to care for children where people try to work out whether they will have to try to re-consent. This is mostly historic data. It is not the gathering of new data, so you do not have the opportunity to seek a new consent; you have to go back and contact people who may not have remembered or may not care. We need balance in whether or not it is something they want to see, so we need a lot more conversation about it.

Q142 Valerie Vaz: People may not have consented, even if they are children. That is the key concern.

Professor Montgomery: Their parents may have consented on their behalf; they may have consented thinking that their consent was abandoning any further involvement, because they were quite happy to put a blood sample into a process. We do not know the answer to those questions.

Q143 Valerie Vaz: I was right in the middle of the inquiry on care.data, so I know the difficulties. Some of the data was released without consent and sold off. What is your view of the EU regulations?

Chris Combemale: It is quite difficult to have a final view because at the moment there are three versions of the legislation: the Parliament version, the Commission version and the Council of Ministers version. They all differ quite considerably on different key clauses. We think the Council of Ministers version gets a better balance between risk and principles versus being prescriptive, and in a fast-changing world things that allow risk-based principles to be incorporated are better. On issues like profiling, we think the Commission and Council versions are both better than the Parliament version because they restrict limitations on profiling to automated profiling that would have a legal effect on the person, whereas the Parliament version asks for consent to every profiling action that might be taken, which from a consumer and marketing point of view would be quite difficult. We know that consumers want relevance; they want products and services that match their purchase history. I think it is right to restrict the limitations on profile to things that have a legal effect and are automated: for instance, automatic approvals of mortgage applications without the intervention of a loan officer. It is highly sensible that you cannot make an automated decision that has a legal effect without the involvement in some way of a human being reviewing that, but the Parliament version goes too far. I do not want to take you through every key clause, but I do not think they have the balance quite right yet. The negotiations are ongoing. We don't really know, because it is behind closed doors, exactly what the final version will be, but from what we understand we think there is movement towards a better balance than some of what existed in the parliamentary version.

Renate Samson: Likewise. There is still a long way to go. I am trying to get my head around it all. A lot of good and interesting conversations are taking place. I am particularly enthused to see a conversation about privacy by design or privacy by default. That is hugely important as we move along in the internet of things. Considering privacy and security at the very start of research and development does not happen now; it is often the afterthought. You have a great idea and then you think, "Oh, crumbs. This might happen." It needs to be the first thing. It should be seen not as a negative but as an opportunity for great innovation. Security does not have to be a bad thing. Security is a good thing, so I am encouraged that it is on the agenda. Likewise, there is still a lot of discussion to go; the trial or the process is not over. I am sure it will not be 100% perfect, but we are definitely thinking more about the citizen.

Professor Montgomery: You made a point about care.data. I am not sure that was care.data, because care.data was never implemented, but in the piece of work Sir Nick Partridge did for the Health and Social Care Information Centre the particular thing that struck me was not that there were no governance processes in place at the initial transfer—contracts were in place—but that there was no ability to see whether contracts were being honoured. The difficulty was that if you looked just at the point of collection it looked as though it was a robust system, but in the way it was implemented we could not tell whether those agreements were honoured. We can speculate that they probably were not honoured in some cases. It is part of our thinking—just focusing on the point at which I agree or do not agree is not enough to protect my interests. There needs to be more than that.

Q144 Valerie Vaz: Can I take it a bit further? There is the idea that we have very good data protection—we have the seven pillars—but maybe the US does not have as robust a system as we do. How do you see the new regulations impacting on, say, companies that do not operate here? They may have some form of base in the EU but they are not based here. How will that impact on companies in different parts of the world?

Renate Samson: That is a very good question that is tricky to answer right now in light of the recent safe harbour situation. I hope conversations are taking place with regard to mutual legal assistance treaties. I understand there are provisions in the conversations about the new data regulations that will look at the US and organisations who engage with Europe. It is being discussed, but I am not in a position to be able to expand on that.

Chair: We will adjourn until we are quorate after the vote and then we will move on to the next panel. Thank you very much, panel, for the time you have given us. It has been fascinating.

Sitting suspended for a Division in the House.

Examination of Witness

Witness: **Christopher Graham,** Information Commissioner, gave evidence.

Q145 Chair: Commissioner, thank you so much for coming to speak to us today. You sat very patiently while we heard from the previous panel. I am sure that you will have some opinions about what they had to say. Your position is a public-facing one. First, could you give your opinion about the very contradictory findings of the DMA and Big Brother Watch in terms of the changing attitudes of the public to sharing data? Big Brother Watch claim their researchers found that 46% of people felt they were being harmed by the collection of data by large companies, and 79% were either very or fairly concerned about their privacy online, while the DMA say that between 2012 and 2015 the number of people happy with the amount of personal information being shared increased from 56% to 60%. That is quite a difficult picture for us to understand. Could you help us?

Christopher Graham: Indeed, Chair. Thank you very much for the invitation to give evidence. I listened with interest to your last session. I thought this was going to be a debate about big data. It is obviously a big debate about data, and much more wide-ranging than the impact of the massive analysis of different datasets. The two positions you heard can be reconciled, because research we have done shows that citizens and consumers have great concerns. Whether they are happy or frightened, they simply assert that they feel they have lost control over their personal information. They want to see the regulator on their behalf pressing their rights to protection of their personal information under the law as it stands; and they want to see that law updated to deal with the new phenomena we have heard about—the internet of things, big data and the very creative exploitation of data. You were hearing two sides, but they were not incompatible.

The important issue we have to resolve is how we can assert information rights granted to citizens under the data protection directive 20 years ago, but clearly a bit creaky and out of date given all the developments going on in the data world, and make sure that we do not lose sight of the fact that, even though the rules of the game have changed in terms of the technology, the rules have not changed. You do not have to abandon the data protection principles in order to make big data work. With big data, there are tremendous benefits to be had, for example in the delivery of public services. If different agencies are able to talk to one another and inferences can be drawn about the mass, clearly that is interesting, but we must not decide that that simply changes the rules of the game to such an extent that privacy and the rights of citizens no longer matter. We can have both the benefits and the rights, provided data controllers think through the implications of what they are proposing and, as we heard from the last session, do proper privacy impact assessments and think about privacy at the outset. That way it is a win-win; we can have better public services, a better health service and more targeted delivery of services without having to accept that you will get discrimination, differential pricing and all the bad things that could follow if we get big data wrong.

Q146 Chair: Some of the evidence we heard from the previous panel was that increasing awareness about what was happening to data and the purposes for which it was being used was behind some of the changes in attitudes. I notice from your written evidence that you have made clear recommendations about including education on a risk-based approach to data protection not only in HE but in the school curriculum to raise schoolchildren's awareness about data privacy. Could you explain that a little?

Christopher Graham: We have been delivering lesson plans for primary and secondary schools about information rights, both data protection and freedom of information. We have been developing those over the past two years, with good advice to make sure they are compatible with the national curriculum and that they deliver appropriate tools for teachers working with different key stages. We want to extend that work into further and higher education. I think the point was very well made that the very inventive people who are working on new products and applications need to understand what the implications of what they are doing might be. They almost need to understand as citizens and consumers the implications of what they are doing, so that they can build in appropriate privacy at the design stage. It is educating both consumers and developers.

Q147 Chair: What would be your assessment of current levels of awareness among young people of data privacy issues?

Christopher Graham: I think it is growing. There is a myth that happy-go-lucky teenagers don't care about their privacy. Because they tend to know more about apps than the rest of us, they are probably more savvy both about the technology and the implications. I am told there are all sorts of applications that people of my generation would think are quite leading edge but are so last year that the kids are on to something else that has more security built into it. There is perhaps a tendency to let too much hang out on social networking sites that people might live to regret later on when they are applying for jobs, but that is just the process of growing up. In terms of understanding what permissions you can give and what permissions you can withhold, each generation gets a little smarter than the last.

Q148 Matt Warman: I am sorry I came in slightly late. Could you lay out a little bit about where you see the role of the ICO at the moment and where you see it when you have what is likely to be a whole load of legislation coming through from Europe in the nearish future in some form or other, and also from this place?

Christopher Graham: If you asked me to characterise the ICO at the moment, I would say fighting on all fronts. We are responsible for the right to privacy but also the right to know. You are looking at the data protection side of my business. I am also concerned about the freedom of information side and the interaction between the two. We are working very hard in such areas as nuisance phone calls and aggressive charity fundraising. Issues have been raised about the development of care.data and the treatment of data in the health service. Every week there seems to be a horror story at the top of my pile, and my investigation team and my enforcement team, which is being expanded, has more and more work to do. I am not complaining; it is an exciting job to do at the moment, but you are quite right to flag the fact that the general data protection regulation is coming down the track from Brussels. They are taking their time about it, but we believe we will see an agreement next year. The job of the Information Commissioner's Office over the two-year period of transition to the new rules is to be there for data controllers and data subjects so that everyone understands what the new rules are.

My organisation is very clear that we are going to have to change to respond to the new responsibilities, and we are standing on the diving board ready to go. It is taking a long time for those rules to be finalised. We are very much involved in the Article 29 Working

Party in Brussels in that debate. There are things we like about the proposed changes and things we do not like, but there is still some way to go. Whether the Luxembourg presidency is going to finalise it or whether it will fall to the Dutch I do not know, but by the middle of next year we will know exactly where we are in that area. Life is never dull at the ICO, but it is particularly not dull at the moment.

Q149 Matt Warman: You mentioned a couple of recent high-profile cases. TalkTalk have now said that perhaps they had not taken all the precautions they could. Does the simple fact of getting hacked mean that you are in breach of the regulations that it is your job to oversee?

Christopher Graham: Every data controller has an obligation under the data protection principles to have in place appropriate technical and organisational measures to protect against unauthorised and unlawful processing. I am quoting from the data protection principles. When a data breach is notified to us, or we discover one, it is our job to investigate. That is what we are doing at the moment, so I must not comment further than that. I think your colleagues on the Culture, Media and Sport Committee will want to have a look at this issue as well.

It is very important that the Information Commissioner is patrolling to make sure that data controllers are sticking to the rules. When something goes wrong, for whatever reason, we need to investigate and, if appropriate, use the powers Parliament has given us either to require undertakings or impose enforcement notices, or it may be appropriate to issue a civil monetary penalty. We have heard that the commissioner has the power to issue civil monetary penalties of up to £500,000 for the most egregious breaches of the data protection principles. I must not jump too far down the track. If it turned out to be bad actors, as they say in Brussels, the criminal sanction would come in, as was discussed in the last session. We will have to wait and see.

Q150 Matt Warman: Do you have data on the percentage of cases you look at where appropriate precautions were taken, so we should not be thinking about fining people who have been hacked—we should be treating them largely as victims of crime?

Christopher Graham: I noticed that TalkTalk were very quick to cast themselves as the victims—within the first 24 hours—and I cannot comment on that until we have completed the investigation. I can certainly get the Committee some statistics on the results of various investigations we have undertaken, to draw the general rather than the particular. In a situation like this the victims are the consumers whose details have been lost. An investigation I can talk about was a travel website earlier this year. We instituted a civil monetary penalty of about £130,000 because 5,000 consumer credit card details had been sold. We discovered that that company had put at risk the credit card numbers, security codes and signatures of 100,000 consumers, so if we are talking about victims those were certainly victims. That was why we imposed a civil monetary penalty. We have the powers to act where we can establish that it is the data controller who has gone wrong, but as far as TalkTalk is concerned we will have to wait until we have finished the investigation.

Q151 Matt Warman: I am trying to get a sense of how many data controllers you encounter who have been hacked despite not having gone wrong. They met a reasonable bar for securing people's data, yet the criminals won the game.

Christopher Graham: I will have to get precise figures for you, but everyone has to accept that hackers are testing, testing, testing. It is a counsel of defeat to say you can never be secure. You can be more secure than you were last year, and you probably have to be. This has been a wake-up call for everybody. You have to put in place the most effective systems you can to make sure that customer information, which has been entrusted to companies, is looked after. The travel insurer I referred to was Staysure. We imposed a civil monetary penalty of £175,000 earlier this year. That is part of the wake-up call. A more effective wake-up call is simply for companies to look at what it does to their brand and their business. I am sure people in TalkTalk are very concerned about the number of people who will not be renewing their contracts with the company as a result of what has happened.

Q152 Matt Warman: You talked about being more secure than last year and getting better. How do you assess what is an adequate level of security? Is it done on a case-by-case basis, or is there a standard evolving that at any given moment is fixed in time?

Christopher Graham: We undertake a lot of audit work to help data controllers get things right. We are not there to catch people out. Last year we conducted 41 full audits and 17 information risk reviews, and we followed up on 56 other audits to make sure our recommendations had been followed through. That is the Information Commissioner being helpful. In the case I just quoted, Staysure, we discovered that the company had been keeping the security code information together with the credit card information. That was a straight breach of the rules, so it was not very difficult to work out that a civil monetary penalty was appropriate. You asked about the proportion of good guys and bad guys. I can get you that information. I do not have those statistics in front of me.

Q153 Carol Monaghan: Can I ask you a bit more about the consent side of data protection? In your submission, you say you envisage organisations facing problems in obtaining consent being able to apply other conditions in the Data Protection Act in order to legitimise the data processing. When might that sort of approach be appropriate?

Christopher Graham: The eight data protection principles, as opposed to the seven pillars, set out the rules under which data can be processed under the data protection directive and the Data Protection Act which stems from that. The first principle is that data must be processed fairly in accordance with the rights and expectations of citizens. Then there is a series of conditions that would enable you to process information, but always subject to that fairness test.

One model is what the Americans call advice and consent; another model, which is also one of the principles, is what is called legitimate interests. If a company in the big data business, for example, is mashing this dataset with that dataset to predict behaviour and all sorts of weird and wonderful things and they are claiming to do that because they have a legitimate interest in doing it, and therefore they are not seeking consent, they have to be able to show that that is not at odds with the rights and freedoms of data subjects and the

principles of fair processing. If you are going to claim legitimate interest, you really have to be able to make it clear to citizens and consumers what you are doing—what the deal is—and why you are doing it. That is where the privacy impact assessment comes in—at the very basic level of design of the project.

When we published our paper on big data last year, our concern was that there were people out there who believed that computer science was so wonderful that we had moved into a 21st/22nd century model and, hey, the boring old Data Protection Act did not apply because it did not work; it was so last year. This is a very dangerous principle. You can still make the data protection principles apply if you apply them at the outset and think it through. It is obviously not going to be possible to get consent for every possible element in some big data mash-up that will give you predictive behaviour, but that may not be necessary. If, however, you simply go ahead and say, "Hey, we're doing this because that's what we can do," you will be in trouble. You will be in trouble with the regulator, you will be in trouble with the law and you will also be in trouble with citizens and consumers, who will go off organisations that treat them in such a cavalier way. I do not think it is binary—that it has to be consent or it has to be legitimate interest. All I would say is that where data controllers are relying on legitimate interest they have to be careful, because it may not work if you have been so tricksy that consumers and citizens do not understand what you are doing and do not like it.

Q154 Carol Monaghan: Is there a danger that as big data brings different datasets together consent will be increasingly compromised?

Christopher Graham: I am saying that it is possible to do most big data projects within the provisions of the Data Protection Act and the eight data protection principles. It is possible if you design things the right way. If you are cavalier about it and do not try, you will get caught out. I am not saying that consent is never appropriate. In certain circumstances, consent will not be possible, in which case you have to have a very compelling argument why you have a legitimate interest that does not interfere with the rights and freedoms of citizens.

Q155 Carol Monaghan: In terms of regulation, what can be done to make privacy notices, terms and conditions, tick boxes and so on, a meaningful way of gaining consent?

Christopher Graham: A lot. Whether or not it involves gaining consent at the end of the day, you need to explain to your users what you are doing. It would help if privacy notices were written in English. It would help if privacy notices were not written by lawyers whose major interest is minding the back of the company; it would help if they were not the length of some of William Shakespeare's longest dramas; and it would help if they were written on the principle that they might not actually be read, rather than people saying they do not have time for it and just pressing the button.

We have done a lot of work with Google, for example. Since Google introduced their new privacy policy in 2012, without so much as a by your leave, we have been very much on their case. Working with Google, we have got them to develop a layered approach to their privacy notice so that you can get more information about what they are doing and proposing. We have moved Google from a privacy statement as long as your arm, full of

boring lawyer stuff, to something that is much more interesting, user-friendly and, frankly, used. You have probably noticed, if you use Google services, that these things pop up and they are rather more informative. In some cases that leads to, "Do you want to use this service? Do you or do you not want to tick this box?", but where an organisation is claiming the right under the Data Protection Act to do what they are doing because of legitimate interest they still have to explain, and they have to be more innovative in evolving ways of explaining what they are doing than data protection lawyers have traditionally come up with.

Q156 Carol Monaghan: Can you require them to be revised and improved?

Christopher Graham: We start off by advising. If people wilfully do not take our advice and an issue arises, we can get into enforcement mode. We have a good code of practice on privacy notices. We are revising that at the moment because of recent developments in technology, and in privacy notices too, and we will be consulting on that shortly. Where it comes to our attention that a data controller is doing tricky things, is not making things clear, or has a downright misleading privacy policy, that can certainly involve enforcement action which, after all, is what we were doing with Google. There are ways and ways of doing enforcement. We are interested in a way of doing enforcement that gets a result that is of benefit to consumers, rather than just getting off on civil monetary penalties.

Q157 Carol Monaghan: So you can.

Christopher Graham: Yes, we can.

Q158 Chair: What is your response to the comments by the Nuffield Council on Bioethics about historical medical data, and the challenges of informed consent by those who gave consent a long time ago for their data to be used for one purpose and that data might now be repurposed?

Christopher Graham: We have been very concerned by what we learned about what has been going on in the health sector. We are engaging very closely with the Health and Social Care Information Centre. I had a meeting the week before last with Dame Fiona Caldicott. The health sector is of huge concern to the Information Commissioner. We want to make sure that we do not get the nonsense of people's personal medical data being used for purposes they had no idea about. We are particularly concerned about information given to GP surgeries or pharmacies landing up in quite inappropriate hands. We had a recent civil monetary penalty against the pharmacy firm Pharmacy2U. We imposed a civil monetary penalty of £130,000, because information given in good faith to the local chemist was landing up in an Australian lottery scam and with the purveyor of a herbal remedy who had been in trouble with the Advertising Standards Authority for unfortunate promotions.

We are also working closely to try to clear up the mess after care.data. The Information Commissioner is sufficiently imaginative to see the power of big data in medical research and in the delivery of health services in the most efficient way possible for the benefit of

patients and the taxpayer. If we can play our part in that we certainly want to, but we want to see things done in the right way so that people's fundamental rights and privacy are not trashed in the name of some higher obligation to efficiency and the onward march of science.

Q159 Jim Dowd: Before we move away from privacy notices, for want of something better to do I clicked on my Sky box which told me to read the details of its software licence. It ran to 102 pages. Needless to say I did not read them, and I am sure nobody ever has.

Christopher Graham: That is the bit I do not usually admit to.

Q160 Jim Dowd: Incidentally, where do all the proceeds of these fines go?

Christopher Graham: Not me. The Chancellor—the contingency, I mean the consolidated fund; it may be the contingency fund, I don't know. I am not incentivised to impose civil monetary penalties. Indeed, I do not even get paid the legal expenses of going after the miscreants, but it is a very useful tool in our toolbox of enforcement powers.

Q161 Jim Dowd: Do you get much resistance to paying?

Christopher Graham: We have had cases where suddenly the company finds it has gone bust and cannot pay, or it goes into liquidation and emerges the next day as something else but very similar. We are in an interesting field.

One of the recommendations that I hope might emerge from your inquiry was touched on in the last session. That is the annoying inability of whoever it is to press the button to start the possibility of a custodial penalty for criminal breaches of the Data Protection Act. That is where individuals go rogue and, without the consent of the data controller, decide to sell information to claims management companies, do the dirty on their ex-wife or something else. At the moment these cases just land up in the magistrates court and it is a fine-only regime. I say "at the moment", but actually you passed legislation in the Criminal Justice and Immigration Act 2008 to provide for the possibility of a custodial penalty, but it has never been commenced. It is section 77 of the Criminal Justice and Immigration Act 2008. If you decide to recommend that it be commenced, it could deal with people who make £30,000 by selling car hire information to lawyers after crashes and so on and land up in the magistrates court being fined just a few thousand pounds. If you decided to make that recommendation, you would be in the illustrious company, as the previous witnesses said, of the Joint Committee on the Communications Data Bill, the Home Affairs Committee, the Justice Committee and the Culture, Media and Sport Committee. One more push and it might actually happen.

Q162 Jim Dowd: I think the report will contain a lot of recommendations by the time we finish. You say in your submission that fairness is a key principle in the Data Protection Act, and that gaining meaningful consent from people is an important part of that fairness. You also indicate that it could lead to profiling and discrimination if left unchecked. Could you give us an example of how that might arise?

Christopher Graham: If we are talking big data, when it is really big it is potentially very useful. When it gets down to granularity it is dealing with personal information. Very often, big data is not dealing with personal information; as a previous witness pointed out, in the example of the advertising hoarding that was taking flight information and meteorological information, that is not personal information, so it is not covered by the Data Protection Act. Very often, big data projects which deal with massive datasets may be dealing with anonymised information. That is not personal information. Where it is dealing with personal information, the smaller it gets, the more potentially problematic it can be, particularly where inferences are being drawn about individuals' behaviour that are to their disadvantage: for example, differential pricing. If I get a worse deal than you online because of all sorts of inferences drawn about my purchasing behaviour, that is not fair. The eight data protection principles, as I have explained are very clear: it has to be fair. Whatever other condition of processing enables you to continue to do that, whether it is consent, in which case the responsibility lies with the data subject, or it is legitimate interest, in which case the responsibility lies with the controller, it has to be fair. If it ain't fair, it's not legal, and that is where the regulator comes in.

Q163 Jim Dowd: In order to sustain fairness in this area, do you think it may be necessary to ban certain types of data processing that profiles individuals to their disadvantage?

Christopher Graham: I do not think one can generalise, nor need one generalise. The law is clear that it is a breach of the first data protection principle if the processing is not fair and is not in line with data subjects' rights under the legislation. That is where the ICO comes in. You do not have to say, "We don't like this category, that category and that category." The circumstances of the processing will lead to the offence, if there is an offence. In the same way, we say to data controllers that, if they are planning a big data project, they should think through the privacy implications right from the start and conduct a privacy impact assessment, just as you would a risk assessment, a PRINCE2 project management or whatever it is. These days you have to do the privacy side as well. If you do not and you get it wrong, you will be in trouble with an information commissioner who, at the moment, has power to impose civil monetary penalties of up to £500,000 and trash your reputation. Under the new regulation being forged in Brussels, data protection authorities across the European Union will have the potential to impose civil monetary penalties based on a percentage of global turnover, which will make even the Googles of this world sit up and take notice.

Q164 Derek Thomas: When data are reused, is it your job to prove that the original consent no longer applies, or is it the job of the person who has the data to prove that the consent still applies?

Christopher Graham: It is the latter. If you acquire a list and you are going to use it as part of your processing operation, you are the data controller because you bought the information. You have to satisfy yourself that, if the person selling it to you says there is consent, there really is consent. The lead generator and list broker businesses are an area ripe for investigation. I would like the power to make an assessment, as we say: a power of non-consensual audit over some of these guys who, particularly in the nuisance phone call and the high-pressure charity fund-raising businesses, are doing all sorts of interesting

things I would like to investigate. I cannot do that unless I get a court order, which I will get only if I have reason to believe things are going wrong or I am invited in, and that does not happen very often. It is not the responsibility of the Information Commissioner to prove that there was not consent; it is the responsibility of the data controller or the data processor to prove that there was. In some of the interesting cases we are looking at now it is very difficult to see where there is any evidence that consent was given. Even if consent was given for the original purpose, do the data subjects whose information is being traded have any idea what is happening to their information? Where is it going? Have they given permission for it to be used for another purpose? I suspect not.

Q165 Derek Thomas: We have talked about bringing together different datasets to find new insights. That has raised concerns that in the case of previously anonymised data we can now identify to whom the data belong. How do you police that?

Christopher Graham: We are doing a lot of work on anonymisation. We have put money in to help fund the UK anonymisation network, which is full of clever computer scientists working out unbreakable codes. We have also published a code of practice on anonymisation. We want to get people to think. A lot of the cases quoted to us are fairly simple things where you mash this and that and you can identify people, but for progress to be made, for example, in very sensitive areas of medical care, you do not need to know who it is you are dealing with; it is just an instance of a particular habit of prescribing, a medical condition and so on. If people are to have confidence that their data can be used for a beneficial purpose, they have to be jolly sure that it will not have a code that can easily be cracked. Anonymisation is very important, and the Information Commissioner's Office thought it worthwhile to invest real money to get that debate going.

Q166 Victoria Borwick: Following on from your code of practice and privacy impact assessments, have you been able to establish how fully and widely they are being used?

Christopher Graham: We are fairly optimistic. We started talking about privacy impact assessments a few years ago, building on work developed by one of the commissioners in North America about privacy by design. In 2014 we produced a code of practice where we specifically made the link between other methodologies, such as PRINCE2, so that it did not feel alien for people working on projects to build it into their project management scheme. We are also building on research we commissioned in 2013 from an outfit called Trilateral, which found there was pretty good take-up—I need to send you the figures that support this assertion—and awareness of the need for privacy impact assessments. Given the very high-profile breaches in recent months, people would need to be very deaf not to realise that that is one of the things the Information Commissioner is looking for when he comes to call. I am reasonably optimistic.

It is clearly a win-win moving forward, because if you are looking at big data—rubbish in, rubbish out—you want good data to be able to draw correct inferences from the datasets you mash. Similarly, the commercial players need trust. Indeed, the Government need trust. If you are to roll out something like care.data in the health sector, there is a lot of ground to be made up and a lot of trust to be won. It raises confidence if people rolling out projects can show that they have considered the privacy side of what needs to be done, in order to win the confidence without which you simply cannot make these projects work.

Q167 Victoria Borwick: Do you wait for the data protection cases to be referred to you for investigation, or do you proactively audit?

Christopher Graham: It is a bit of both. We learn a lot from complaints. Complaints to us are data. That is how we have managed to make some of the big breakthroughs in the nuisance call business. People have taken the trouble to report on the Information Commissioner's website, so we have leads and we can see patterns building up and work out who the bad actors are.

Q168 Victoria Borwick: That is about the constant repeat calls we all get, for protection insurance or whatever it is called, however many times you press delete, delete, delete.

Christopher Graham: Yes. A gratifyingly large number of people go on to the ICO website to report concerns about nuisance phone calls. They say, "These are the people who rang me, this is what they said, this is when it was and this is the number." That has enabled us, for example, to execute a couple of warrants in Trafford and Hove where we found warehouses full of mobile phones with prepaid SIM cards just dialling up numbers.

Q169 Victoria Borwick: That is very valuable.

Christopher Graham: We are also doing a bit of mystery shopping. You ask whether we just wait for complaints to come in. No, we do not; we go out and buy our own prepaid SIM cards and see what calls we get. We log the information and act upon it. We also do a lot of proactive audit and advice work, not to catch people out but to help people to do things better. It is a combination of active and passive that helps us to deliver.

Q170 Victoria Borwick: It is very valuable to know that. Part of the role of this Committee is to inform and make sure people understand. It reminds people that it is available to them when they hear it said today on the web, so to tell us that is really valuable. Are there particular sectors that you think are worse than others? Is the public or private sector worse? What about local or central Government? Do you have particular areas of concern? You have kindly touched on some today.

Christopher Graham: I have a continuing concern about local government. I know everyone is working very hard in local government and they are suffering cuts, but local government deals with some of the most sensitive information, after the health sector. In the health sector I recently got the power of non-consensual audit. I think I should have the same for local government. Local government deals with social care; increasingly, it is dealing with the join-up between the health service and social care. In Greater Manchester, it is going to be in charge of the NHS. It is illogical to have responsibility for the NHS in terms of having the power of non-consensual audit when the NHS is the NHS, but as soon as it is the northern powerhouse I do not have that power. I have great hopes that the new Secretary of State will listen to the very logical case that, if I have that power in the health sector, I also ought to have it for local government.

Q171 Chris Green: The ICO is developing a privacy seal. How do you envisage that working?

Christopher Graham: The idea of a privacy seal is that it is beyond the ISO standard; it is something people can recognise as a good housekeeping seal of approval on sites that sign up to doing things properly, and are prepared to be audited for doing that. I do not want it to be an ICO symbol, because I reserve the right to investigate complaints, even in the case of those proudly carrying the badge. We have to develop a different brand and it has to be one that conveys something to consumers and is recognisable, so there is a good piece of marketing work going on at the moment.

What we want to do then is identify scheme operators who can apply that brand independently of the ICO—operators who have been accredited by the UK Accreditation Service. It is a very carefully designed project. We envisage that at the beginning of next year we will be able to advertise for scheme operators. When we have the scheme operators in place the following year, in 2017, you will see that good housekeeping seal of approval. I think that will give consumers a way of recognising that this is a serious player that understands privacy and is committed to looking after their data. That will give those companies a competitive advantage.

Q172 Chris Green: We heard earlier about a relationship developing between the service provider and the user, and that whenever the relationship is changed by the service provider you can approve and say, "Yes, I agree to this." We could imagine that, if we have a whole range of different relationships with different service providers, having to agree to these things time and time again could become quite a burden.

Christopher Graham: Yes—or not.

Q173 Chris Green: With a kitemark or a privacy seal, we could say, "I am comfortable with this company because they have a privacy seal. I do not need to read all these documents."

Christopher Graham: You still have to make choices, don't you? I hope the privacy seal will help to sort out the people who take it seriously from the people who couldn't care less, but at any time companies are entitled to offer a different proposition. At the moment, my bank is putting to me a different proposition about my account and my credit card. I will decide whether I am interested in that. If not, I will take my business elsewhere. That is not about privacy; it is just that this is the deal. You were getting points; now you will not get them but something else. I need to think about that. As intelligent consumers we always need to consider choices, but what we do not want are phoney choices foisted on us with just, "Here's a load of legal blah, which you won't have time to read, but, hey, press the button and off we go." Then you find that you have signed away your rights. The example I like to quote is the No. 88 bus, which runs between Altringham and Wilmslow and provides a wonderful wi-fi service. At least I thought it was wonderful until I looked at the privacy notice. The last time I looked it said, "Privacy notice: to be posted when agreed." I did not find that very reassuring and—tell you what—I do not use the service.

Q174 Chris Green: If you see the kitemark, whatever form it takes, you would have a certain level of trust that the relationship is quite reasonable and normal.

Christopher Graham: Yes. If my bus company by a miracle got the seal and then was not providing a privacy service, it would pretty quickly lose that seal.

Q175 Chris Green: The European Union is developing a kitemark with the EU data protection regulation. Will the privacy mark be compatible with that?

Christopher Graham: Yes, and we are ahead of the game. It is one of the things that I think is in all three drafts. The Parliament, the Council and the Commission drafts talk about encouraging accreditation seals, so we are confident that ours will work under the new rules. Ours will be in place about two years before the regulation comes down the track.

Q176 Dr Mathias: In your submission you talked about wanting the introduction of a criminal offence for breaches of the Data Protection Act. Why is that necessary, especially when you have been talking about the existing Criminal Justice and Immigration Act? Can you expand on that?

Christopher Graham: My major concern is that section 77 has not been commenced yet, as you know. By the way, there is section 78 as well; it provides a defence for investigative journalists who might be caught up in this, so sections 77 and 78 both need to be commenced together. There is a criminal penalty for breaches of the Data Protection Act, but it may be that in this world of big data we need to extend that a little to deal with the problem of the de-anonymisation of datasets, which was mentioned. If some malicious troll—

Q177 Dr Mathias: Are you saying that section does not cover it?

Christopher Graham: Section 55 just deals with the unauthorised obtaining or disclosure of personal information without the knowledge of the data controller. I would not like to test a de-anonymisation or re-identification case against that. It is worth floating the idea that, in the same way as the 20-year-old directive needs updating because of developments in the digital economy and big data, possibly the Data Protection Act needs updating too. Of course, the Data Protection Act is the way in which the directive was transposed into UK law, so it probably needs a bit of a tinker as well.

Q178 Dr Mathias: What concerns me is that you are saying the legislation is not specific enough, yet if you make it too specific you will need to create more laws. Would that be right?

Christopher Graham: We could proceed immediately. I know that primary legislation takes for ever, and I cannot imagine that the Government would want to embark on a revision of the Data Protection Act until we know what the regulation says. Nothing is going to happen until the next Session of Parliament at the earliest, but the commencement of sections 77 and 78 of the 2008 Act could and should happen in very short order,

because one of the ways in which you can rebuild confidence after the care.data fiasco, for example, is to reassure people about their pharmacy, GP and car information, if it goes AWOL not because the data controller got something wrong but because somebody just decided to do something bad. That is not about a civil monetary penalty; that is about taking people to court.

At the risk of boring you, the problem is that when you get to court the fine will always be based on your ability to pay. If you have just been sacked, it is very easy to make the case that you have no means, so the fine will be very modest, and even if you made £35,000 by the scam you will still be fined a paltry sum. You need to have in the back of your head, "This is serious. I could go to prison. It's not worth it; I won't go there." That would raise the profile of the whole concern about privacy and data protection.

I am not one of those people who believes in banging up everybody—I am sure you aren't either—but it never says that you might possibly go to prison, or there is anything between a fine of 400 quid and anything else, or the possibility of a suspended sentence or community punishment. My people investigating these activities cannot require people to attend interview because it is not a recordable offence. All this stuff is just basic, surely. This Committee is looking at the really difficult stuff of big data and the future. Here we have a little piece of legislation that nobody has got round to commencing yet, and which is absolutely fundamental to protecting privacy and instilling good data protection principles before we ever get to any of the difficult stuff.

Q179 Valerie Vaz: Has that stopped you or prevented you taking cases further?

Christopher Graham: I take cases before magistrates courts and I weep when the fine is £250 and a £100 community sentence, but it does not stop me taking the cases. It does not provide the deterrent that I want. We will continue, but it would make our investigations much easier if I could require people to attend for interview rather than asking them nicely. It would make the investigations quicker. If the offences were recordable and on the police national computer, that itself is a disincentive.

Q180 Valerie Vaz: You and some of my colleagues have touched on the regulations that are being looked at. For the record, where are we with the regulations? Presumably, you have been involved in them and in a number of issues coming up. I mentioned some of them earlier: the right to be forgotten and the reference to 5% of turnover, which I think would be helpful to you in the case of some of the bigger companies. Where are you on some of the main enactments that they are looking at?

Christopher Graham: Our position is that it is a bit of a curate's egg—good in parts. The bits we like are where there are enhanced and relevant powers and rights for data subjects and data portability—very often access to data in digital form. We heard about the midata project. That is being legislated for. Data portability is really more relevant than the right to be forgotten. It is not really a right to be forgotten; it is a right to be de-listed, if you like, or a right to be a little more anonymous so that in certain circumstances you cannot have searches on your name that produce all sorts of outdated and irrelevant information, or spent convictions which may be outdated and irrelevant. We like the stronger fining powers for data protection authorities. As to whether it is up to 5% of global turnover, we

will see. What I do not like is the lack of discretion I would have as a data protection authority. It is no good the text saying that, in the event of this, this and this happening, the data protection authority shall impose a fine of up to such and such. Better regulation is about having discretion and deciding which tools to employ. I am told that what it actually means is that you would only have to fine €1. Well, excuse me. It is not worth going through all the legal rumpty-too to fine €1. Credit us with a bit of common sense and leave it to data protection authorities to decide on the best tools to use in order to secure compliance. That is an example of the way in which the regulation in its various forms is rather over-specced. It is as if every good practice example has been thrown into the pot and then legislated for. We won't be able to move for all these very specific obligations that are a bit box-ticking. I am hoping that over the next few months it will lighten up a bit.

We know that the ICO will have to change. I do not want it to have to change to be just a circumlocution office, if you like, for the new regulation. We also remain to be convinced that the detail of the one-stop shop has been thought through. A one-stop shop is a great idea if you have cases being pursued across all the member states in different ways. That is a waste of everybody's time and it is an annoyance for the big players. If you are to have a one-stop shop, have it, but a one-stop-shop that then has to involve all the data protection authorities with rights to appeal in all the national courts is what I have described as a one-stop shop with a branch in every town. It is really not worth having.

We recognise that it is a game changer and will be a huge task for the ICO. We have a major task to inform industry and public authorities how they will have to change to comply. That will fall to my successor, not me. It is very important that Whitehall gets on with the business of pressing the starting button on the recruitment of my successor, because I run out of road at midnight on 28 June next year. We need the next Information Commissioner to be identified as soon as possible. There is a task for somebody over Christmas.

Q181 Valerie Vaz: That is very sad to hear, because you have been an exemplary information commissioner. I know your term was extended. Do you think the role will change once the new regulations come in? You touched on updating the DPA 1998. Presumably, new legislation will have to be made to incorporate where we are on the technology.

Christopher Graham: Yes. We are readying the ICO for having to move in a different way, but a different way to deliver the same result, which is upholding information rights on behalf of citizens and consumers, making sure that public authorities can do things sufficiently and that industry can thrive, but all sticking to the rules so that the wonderful potential of the digital economy works for all parties and delivers results, and is not based on trickery and the clever guys doing down the ignorant and the big guy doing down the little guy. The Information Commissioner is there to hold the ring. We will do it in a different way and with increased powers. I hope we will do it with increased resources. By abolishing the obligation to notify under the Data Protection Act, the new regulation poses a little problem for me, because that is £18 million of income down the tubes. We have to think of a different way of funding the regulator in fairly short order, which is another

thing to think about over Christmas. There is lots to be done, but we are not daunted. We are raring to go at the ICO; we just want the starting gun to be fired on all this new stuff.

Q182 Valerie Vaz: Do you see a new DPA?

Christopher Graham: There will have to be. The Data Protection Act will have to be amended to take on board the requirements of the regulation, because the regulation will apply. It does not have to be transposed in the same way, but our law will have to flex to accommodate the fact that there is a regulation that applies in all member states. Increasingly, we are dealing with cross-border phenomena. We have to make things work within the European Union and we have to make things work with colleagues right across the globe. There is no point my raging in the UK against some American outfit unless we have good relations with the Federal Trade Commission and other partners. It will be a different job, but a different job delivering the same increasingly important objective of making sure that there is a level playing field and that the fundamental right to data protection and privacy is secured.

Q183 Valerie Vaz: Thank you for waiting while we had a vote. Thank you for all the work you have done.

Christopher Graham: Thank you very much. I still have seven months to go, so don't write me off.

Valerie Vaz: But we might not see you before then.

Q184 Chair: You made a few recommendations to the Committee this afternoon. You mentioned that you do not have audit powers without consent. Is the issue that the threshold at court is too high to make your case, or is it that you want audit powers just within your own statutory basis?

Christopher Graham: There is the power of assessment where the Information Commissioner can come in and have a look at an organisation, but it is by consent. The previous Prime Minister, Gordon Brown, simply said that all Whitehall Departments will be subject to non-consensual audit by the Information Commissioner. Most recently, that right was extended by ministerial order to health service bodies. I am saying that it ought logically to apply to local government as well. I have written to Greg Clark about it, because it is really important. It is about confidence building. If performance needs to be improved in local authorities, we should not have to wait for a car crash. Local authorities need to know that the Information Commissioner could come in and run his eyes over the books; otherwise, I have to wait until something has gone wrong to get an information notice to carry out enforcement work.

Q185 Chair: Are there any other areas of concern or sectors where you do not have the audit powers that you feel you need?

Christopher Graham: There are quite a few. I must not run before I can walk, and there would be a question of resources to do this. I think the lead generator and list broker sector is one where it would be very logical for there to be powers of compulsory audit.

Q186 Chair: We have just been talking about the EU regulation, which is obviously going to have a huge impact on domestic legislation. Give us an idea of your assessment of the timeline for that. We are hearing conflicting reports about when those three versions might become one version and when that might make more progress.

Christopher Graham: Don't hold me to this, because I have lost track of whether it is all going to be sorted out in the Latvian, Luxembourg or Dutch presidency. If things really go wrong it will fall to the UK presidency in the second half of 2017, which nobody seems to be aware of, to sort out. The Luxembourgers are really determined to get a political agreement by the end of the year. Then there will be a bit of to-ing and fro-ing and possibly by late spring the thing will be finalised, but there is then a two-year transition period. That is where you people come in with changes to the Data Protection Act, probably in the next Session, and the Information Commissioner will be charged with the very important matter of helping business, industry and consumers to come to terms with the new rules.

Chair: Commissioner, thank you very much. Valerie Vaz is right. You have been an outstanding commissioner in what has been a challenging time, with data expanding exponentially. I hope you will not allow the challenges of the next few months to keep you too challenged over Christmas and that you enjoy a little bit of Christmas. We may write to you to follow up some of this evidence, and perhaps some of the issues to do with the Investigatory Powers Bill. Thank you very much for your evidence and for waiting patiently.

Christopher Graham: Thank you very much indeed.