HOUSE OF COMMONS

Science and Technology Committee

Oral evidence: Social media data and real time analytics, HC 245

Wednesday 2 July 2014

Ordered by the House of Commons to be published on 2 July 2014.

Written evidence from witnesses:

- Information Commissioner's Office
- University of Manchester
- Dr Kevin Macnish
- Government Departments

Watch the meeting

Members present: Mr Andrew Miller (Chair); Mr David Heath; Stephen Metcalfe; Stephen Mosley; Pamela Nash; Graham Stringer; David Tredinnick

Questions 156-227

Witnesses: **Steve Wood,** Head of Policy Delivery, Information Commissioner's Office, **Dr Mark Elliot**, Senior Lecturer, Confidentiality and Privacy Research Issues group, University of Manchester, and **Dr Kevin Macnish**, Teaching Fellow and Consultant, Inter-Disciplinary Applied Ethics Centre, University of Leeds, gave evidence.

Q156 Chair: Good morning, gentlemen. Thank you for your patience. We have been trying to finalise another report on an entirely different subject, which we hope will become clear in a few days. For the record, I would be grateful if you would introduce yourselves.

Dr Macnish: I am Kevin Macnish from the Inter-Disciplinary Applied Ethics Centre at the University of Leeds.

Steve Wood: I am Steve Wood. I am head of policy delivery at the Information Commissioner's Office.

Dr Elliot: I am Mark Elliot from the School of Social Sciences at the University of Manchester.

Q157 Chair: Some of the witnesses we have heard from and the evidence that has come in have suggested that the use of social media data produces a minefield for ethicists and should be limited until we have very core defined ethical standards in place. Do you agree with that, or do you see that there are problems?

> ***Dr Macnish***: Yes; there are certainly problems with it. The amount of information people are putting out about themselves and the amount of information that can be gained and potentially abused is quite revolutionary. We simply do not have in place the regulations, or even the ethical understanding in many cases, to know how to deal with this.
>
> ***Steve Wood***: From the perspective of the Information Commissioner's Office, we are focused on the regulation of the Data Protection Act and the interaction between this area and personal data. There are certain rules and pieces of legislation in place which interact with this area, but we certainly see a need to modernise the data protection framework. That work is currently taking place in the negotiations in Europe over the new data protection regulations to see how they can be modernised. Equally, we see a welcome interaction between the world of data protection and the wider development of ethics committees, in particular the use of ethical frameworks in the commercial sector, which may be a new approach. We certainly see a welcome interaction between those areas.
>
> ***Dr Elliot***: We do not yet understand the psychology of being in these public/private spaces where there is a fusion of understandings of what is private and what is public. It is clear that something being placed on social media is not a consent to do whatever you want with it now. People's understanding of what they are doing when entering information into a social media site or Twitter is not the same as broadcasting something to be used subsequently for whatever purpose anybody wants to use it for.

Q158 Chair: Dr Elliot, in your evidence you said that, in comparison with other types of data, the ethical guidelines for social media data are underdeveloped. Is that simply because it is also new, or are there barriers that we have not considered in other similar debates?

> ***Dr Elliot***: The newness of it is really important. We are also facing issues where social media data are not used on their own. There is increasingly interest in linking the data to other data, which throws up a whole set of different issues. You cannot take this out of the big data context. Social media data are one type of the new data that are often called big data. How those data fit in with all the other data available for use in various different ways by different groups of people with overlapping interests is something we need to take into account, and that framework is just not there.

Q159 Chair: More generally on this point, we have to try to synthesise a sensible report out of an incredibly complicated set of information that has come to us. Clearly, there are concerns about ethics in this space. If you were assisting us to draft that report, give us one ethical guideline that you think ought to be firmly implanted in our considerations.

> ***Steve Wood***: In terms of the interaction between privacy and data protection issues, one area we are keen to promote is the concept of a privacy impact assessment. I think that can interact quite well with wider ethical considerations, particularly considering the effects and potential use of the data and different range of scenarios, from research to looking at trends and sentiment issues relating to social media, compared with other areas where the data might be used more to create a profile that might be applied, and may relate to

decision making, to an individual, where it may have different types of impact. The privacy impact assessment that we have developed at the Information Commissioner's Office can be a useful tool which can link and work well in the wider context of ethical considerations. So that might be one of my opening points.

Dr Macnish: Speaking as an ethicist, I would say much more broadly than that even, but simply just do no harm as much as possible. It may sound facetious, but a lot of good can come out of social media and big data in general, but there is also tremendous scope for abuse. What we should be looking to do as a community, both in law and in ethics, is to limit that harm to the greatest extent possible while also freeing up the benefits that can come out of it.

Dr Elliot: I think it is defining the principles of what is and is not fair use of the information, and also the relationship between the provider of the social media and the users. The recent report to hit the news headlines about experiments being conducted by Facebook is a clear example of misuse. This goes beyond the data, and that is why it gets so complicated. This is not just about the data; it is about the relationship between Facebook and its users who are being manipulated in the experiment. Clearly, experimental use of information, which is using your data for research, goes beyond that. It is the use of Facebook users for research, and a boundary there has been crossed.

Q160 Stephen Mosley: There is a boundary there, but do you think data protection legislation hinders the legitimate use of data for research?

Steve Wood: I do not think data protection legislation necessarily hinders the use of data for research. It contains a set of principles. As Mark has already mentioned, the first principle relating to fairness is a really useful tool which can guide people to the right considerations, thinking about the reasonable expectations of the data subject and other impacts on them. A lot of the debate has been around the future data protection regulations and the balance between the need to have consent for research and whether other conditions can be used in data protection legislation to legitimise the research, if you like. There has been widespread debate in relation to the proposed data protection regulations being negotiated in Brussels about what that balance should be. At the Information Commissioner's Office we accept that in some circumstances consent will not always be the right route for research for a number of reasons, but there are other conditions and tools which should be available in the legislation to consider whether the research can go ahead. For example, considering the concept of legitimate interest still requires a data controller to take into account the impact on the data subject and to think about the benefits and legitimate reasons why they are doing that research. It is about a balance of the legitimate conditions to focus on the research. Consent has its place, but it is about that balance.

I do not think the current data protection law as it stands is necessarily a barrier to research. Sometimes it can be misunderstood, but, equally, there are issues about getting the balance right to make sure we have the right protections, but, equally, to make sure there is a reasonable understanding and reflecting how research can work in the current data protection legislation.

Q161 Stephen Mosley: Surely, if something has been legitimately published—let's say they are court records, for instance, or an individual has posted it publicly themselves—and it is publicly available, it should be available for research purposes.

> ***Steve Wood***: Yes, and often in those scenarios the research can take place on a legitimate basis. It is thinking through the different implications and scenarios with some of that information, particularly if it is held for a longer period or how the research progresses. It very much depends on the scenario. I think the key piece of information to get to users is to make sure they can understand in clear and transparent terms what the research means for them and how their data is being used. Equally, sometimes there is a misconception that once the data is public it ceases to be personal data. It is still personal data under the legislation; it is just that it has to work through the conditions for the research to be able to take place. The fact that it is public is a factor which often can link in to legitimise the research in the first place.

> ***Dr Macnish***: On the back of what Mark said earlier, there is not the clear public/private divide any more that there might have been 20 years ago. When you publish something on Facebook, your reasonable expectations may be that it just goes out to a very limited number of friends; it may be only 10 people. That might be seen in the sense of almost a personal letter, but in fact you can have personal communications between two people on Facebook. You can make a statement public and then it goes out to everybody, or, when you are using a social media platform like Twitter, everything is public by default, although you can also ban certain people from seeing what you post on Twitter. It is not a straightforward public/private divide. With social media you are talking about a quasi-public arena, which I think muddies the waters quite a bit.

> ***Dr Elliot***: There is a distinction here between "published" and "public." If you have deliberately self-published something—for example, if you post your CV online—you have the obvious intent that people should read it and that is its intention. The same goes for certain sorts of web activity such as blogging. You desire people to come and look at the website. Social media is not quite in that category. It may be public or semi-public, but that is not the same as publishing, which is the deliberate intent to put it out to as many people as possible. There is a grey area here.

Q162 Stephen Mosley: In May, the European court made a judgment on Google and demanded that it removed links. I think these were newspaper articles referring to a court case about 15 years ago. Do you think that sort of thing could be considered as a censorship of data?

> ***Steve Wood***: The first thing I would say about the judgment is that it is not, as some have characterised it, rewriting or deleting history; it is about the removal of the links when they are returned from a search result against an individual's name. The other thing to mention about the court judgment is that it is not an absolute right to be able to go to a search engine and ask for those links to be removed. Essentially, it still has to be an infringement of data protection law, and then a consideration will come into play as well about the status of the information and the relationship of the individual in terms of their public profile in considering freedom of expression issues.

One of the challenges of the judgment, and the issue we are still mulling over, is that it does not make very much reference to freedom of expression. Picking up your point about censorship, it is quite a challenging judgment for us to interpret. The court did not make that much reference to the importance of freedom of expression, but we are still working through the implications to come up with a sensible approach to how we apply that judgment in our work. As the information commissioner responsible for both data protection and freedom of information, we are aware of the importance of both rights.

Dr Macnish: There is a lot of detail to be worked out in the whole concept of the right to be forgotten that the Spanish judgment was drawing on. The principle, at least as stated by the European Parliament at the moment, is that it will not apply to newspaper archives, for instance, but are *Huffington Post* or *Salon.com*—solely online publishers—newspapers? What about an individual person's blog? Some people blog and the information they share is treated extremely seriously, and sometimes even taken more seriously than what might be in the newspapers. For other people, it might just be a blog about their family background. What counts as being a newspaper in that sense is not entirely clear.

Another issue which comes up is the idea that, if it is in the public interest, it should not be deleted. But, again, how do you know whether or not something is in the public interest, especially after a gap of five, 10 or 15 years? It may turn out that something which five years ago is no longer in the public interest in another 10 years' time suddenly does become in the public interest. Let's say a person has a particular political viewpoint which is expressed and gets in the public record. Five years later they say, "I have not been engaging in politics recently. I wish to have that struck off the record," and 10 years later they do get into politics and follow up certain views. For the rest of us, we might think it would be helpful to know what they once expressed in public.

Q163 Stephen Mosley: We keep hearing about the right to be forgotten. An alternative point of view is that there should be a right to be forgiven. Have you heard that term used at all, and, if so, do you think a right to be forgiven might be better than a right to be forgotten?

Steve Wood: We have indicated that the term "right to be forgotten" is quite difficult. It also raises expectations in the public about what might be able to happen. Whether "right to be forgotten" is the right term, it is not one we are wedded to or necessarily promoting as the data protection regulator. There is currently a right to erasure, which is more explicitly in the current data protection regulations. It may be that sticking to those terms is more helpful.

I think the term "right to be forgiven" has been advanced by some US commentators as an alternative concept in US society, but, again, it only takes us so far; it still leads us into some of the difficult issues that Kevin was outlining. I think it is the importance of the term. It is quite a loaded term. It has been advanced by the European Commission under their current proposals for a draft data protection regulation. It is clearly part of setting out a concept, but it may be an unhelpful one in what it gives to users but having some important ideas behind it. The idea behind it is a good one, which is giving users more control over their data. We are supportive of that.

Q164 Mr Heath: Can I explore the concept of informed consent? I accept that you can probably achieve consent, but by the time you have got to the 106th page of the terms and conditions and clicked "I agree" you probably have not been informed a great deal. Is informed consent a conceit? Is it a concept that we can actually make work?

> ***Dr Macnish***: With informed consent, a lot of the question depends on what you are being informed about. I do not think you have to be informed about the exact process your data will go through, or all the legal aspects surrounding it, but it is reasonable to be informed about the risks and benefits that will occur to you as a result of your data having been used. For instance, Facebook has been in the press recently over the use of its wall to manipulate emotions, or at least that is the way it has been presented. One word of research in its 9,400-word terms and conditions seems not to be informed consent by anybody's remote stretch of the imagination. It seems reasonable to suggest that, if you are going to go into some sort of experiment like this, you tell the users, "We are going to engage in an experiment. These are the harms and the benefits that may occur. Do you consent to doing this?"

Q165 Chair: It is a bit like the health warning on a pack of cigarettes.

> ***Dr Macnish***: It is not far off. Universities have been doing this with ethics research boards for quite some time, and it seems quite reasonable to expect that companies should obey the same standards and requirements as universities.

Q166 Mr Heath: Each and every time a piece of information is used for research purposes.

> ***Dr Macnish***: I believe so, yes; yes, I would say so.
>
> ***Dr Elliot***: We—being collectively our society, the science community, business and so on—are not exploring how we could use this technology to obtain consent. Obtaining real time consent is a technical possibility now. We could be asking people explicitly each time we want to use their data for a new purpose, using the very media we are talking about now, using technology that is already existing. There has to be a policy will and investment in infrastructure to do that. One of the logistic barriers for consent has always been that it is too difficult to get in touch with people to ask them whether you can now use their data for an entirely new purpose. That is no longer the case. At the moment there is quite a lot of fabrication about why we are not going forward with this technology. There is a lot of vested interest in the existing way of doing things about holding on to data and doing work on the data that you have got, rather than accessing data when you need it.

Q167 Mr Heath: Dr Elliot, you are suggesting that the technology can provide that explicit case-by-case consent. You would not necessarily need to move, for instance, to identity assurance providers as a way of coping with it.

> ***Dr Elliot***: I said "could"—not "can." I think work still needs to be done to provide the infrastructure for that, but, yes, absolutely it is possible to do that. You could do it in a variety of different ways. Identity assurance providers would be one mechanism by which

you could deliver that; the use of brokers and personal data stores is another approach. We would not necessarily need to do just one thing.

Q168 Mr Heath: As a very basic question, do we know whether people actually want this paraphernalia and this approach? Is there any research that says, yes, people do want to give their informed consent rather than simply have it—

Dr Macnish: Research carried out by Eurobarometer 2011 suggested that 80% of UK citizens were concerned about their data being used by companies without user consent. Ireland also returned an 80% concern. The two countries were the highest in Europe in that regard.

Q169 Mr Heath: Do you have any thoughts as an academic on why the Anglo-Saxons or Celts should be particularly exercised by this?

Dr Macnish: I am not sure. I can hazard a guess on that one.

Q170 Mr Heath: Mr Wood, is there anything you want to add?

Steve Wood: I would support the comments made about the importance of consent and considering different ways we can achieve it. It is also thinking about the level of information that is needed for different types of scenarios. In terms of data protection, we always talk about the level of information increasing, or that the detail or explanation may need to increase. The more intrusive the processing of the data and the greater the risks or implications for the individual, the more important it is that they have very clear information and it is very clearly provided to them, so it works on that scale.

The other thing with regard to consent is that you should use consent only when it is true consent—an individual has a choice and it is freely informed—and there is not an imbalance. That is why we say that sometimes consent is perhaps not always the right option. There may be other ways you need to think about it. I very much echo and support getting away from the idea of having just very long privacy notices which people are struggling to read. They can be 10,000 words long. The idea is sort of just-in-time technology and real time information, and there are some areas developing in mobile apps where we can see that starting to work. There needs to be innovation in both the public and private sectors in getting this information to people, so there are possibilities there which can be explored.

Q171 Mr Heath: Do you expect the regulator to be setting this out or industry to be offering it?

Steve Wood: We have set out some initial guidance in a code of practice on privacy notices which we published in 2010. We are in the process of updating that and consulting industry on it in light of some of these developments such as just-in-time technology. We will provide some guidance. It will not necessarily all be specifically on research; it obviously covers a wide range of circumstances.

Q172 Stephen Metcalfe: Struggling to read 10,000 words is probably the understatement of the century. You just click the box "I agree" and then get to the really interesting stuff. Do you think notices containing tens of thousands of words—I think one has 176,000 words, which is absurd—are deliberately designed to be totally impenetrable so that you do just click "I agree," and all sorts of stuff could be hidden inside it?

> ***Steve Wood***: I would not say they are necessarily written in that way deliberately. Often, they will come from a culture within an organisation where lawyers are heavily involved. It may also be about writing terms and conditions that cover other aspects like terms of sale and so on. It comes from the point of view that you need to cover everything. In part, it comes from that perspective rather than being deliberately long, but there may be some organisations that sometimes are able to exploit the opacity of the notice. There are lots of different techniques to get round it. There is also the concept of a layered notice—I do not know whether you have heard of that before—where you have the basic information at the first point in a privacy notice, perhaps even some symbols and other things to explain it, and there is still more information in the notice for people to drill down. That is the other concept we have been promoting.

Q173 Chair: It is not helped by documents written for American courtrooms and intended to be applied globally.

> ***Steve Wood***: Yes. We recognise there is more to be done, and it is a priority area for us in continuing to explain that. It is also a source of concern in other areas. We receive complaints about nuisance telephone calls where people have not realised what was in the privacy notice and it is argued that they have consented, so it is an important issue to us in a number of different areas.

Q174 Stephen Metcalfe: It is entirely right that it is an important issue. It is that box you just click to get through, and it has huge implications. You said you were putting pressure on to improve it and perhaps adopt a layered approach to terms and conditions. On whom are you putting pressure?

> ***Steve Wood***: In terms of the guidance and the messages we are putting out, saying we have this code of practice on privacy notices. We also promote the concept of what we call privacy by design. One of the improvements in the proposed data protection regulation being negotiated at the moment is the concept of data protection by design and default, which is actually in the legislation. We think it will be helpful in giving us a slightly stronger statutory hook to promote that concept as well. It is a mixture of us providing guidance and working with the industry. We want industry to come up with solutions and ideas about how to do this.

Q175 Stephen Metcalfe: What about getting the public to have a greater understanding that when they click the box "I agree" there are implications to that? How do we go about that?

> ***Steve Wood***: It is an area on which we are seeking to do work to make sure that people are aware of their rights and the importance of interaction with the information they receive. I

think there needs to be a mix of people involved in it; we cannot do it all ourselves. We are increasingly dealing in partnerships and working with other organisations—for example, citizens advice bureaux and organisations like that. We have also started a programme of teaching materials for schools on data protection. It is not just about being safe online; it is more about interactions and young people learning about transactions and about their information. We have had quite a good success rate. Those have been rolled out in primary and secondary education as well, but it is a long process.

Dr Macnish: I would back up what Steve said about schools in particular. I talk to undergraduates about this. We are now getting undergraduates who have been with Facebook since they were 13. I would estimate that about one in 50 has read the terms and conditions on Facebook.

Q176 Stephen Metcalfe: That many.

Dr Macnish: Well, they might just be trying to show off in front of their classmates. Some of them do have concern. However, there is clearly a generation growing up that does not take this seriously and trusts Facebook—I am not picking on them—and other social media with their data. It is a real concern. As Steve said, getting them at school is the place we need to be focusing on, but, if we are going to make the terms and conditions understandable to schoolchildren, that gives us a level of English and understanding that I think is sensible to be aiming at.

Q177 Stephen Metcalfe: So there is still more work to be done in that area.

Dr Macnish: Very much so.

Q178 Stephen Metcalfe: Google's motto, allegedly—there is some issue around it—is "Don't be evil." Can any of the companies that are collecting data live up to that kind of ethos, or, because of the sheer scale of the organisations involved in the data, when they think they are being good, the potential is that they can be doing great harm?

Dr Macnish: "Evil" is a very strong word to use.

Q179 Stephen Metcalfe: It is in inverted commas.

Dr Macnish: Indeed, yes. Rather as I said earlier, the potential for harm is there and is significant. Just because a company's intentions are good it does not follow, therefore, that what it does is right. That information can be abused by others. Function creep can occur, whereby the initial intention is morphed slowly and slowly until eventually you end up in a totally different position that was not envisaged at the beginning. So those initial good intentions suddenly find themselves having some very negative consequences and outcomes.

Q180 Mr Heath: Coming back to the earlier point about the terms and conditions and the American angle to this, it does occur to me that there are 51 jurisdictions in the United States, each one of them asserting extraterritorial jurisdiction as well. So, whatever we do within Europe, companies will still feel the need to protect themselves under US and state law and have these rigmaroles despite our best intentions. Mr Wood, do you know if there are any discussions with the American authorities, and do they take the same view?

> ***Steve Wood***: It is a good point about the global dimension to these issues that we have to seek global solutions and standards ultimately. We work and co-operate a lot in Europe with other data protection authorities under the data protection directive, but increasingly we are working internationally. We have just signed a memorandum of understanding with the Federal Trade Commission—the FTC. There are a lot of discussions now and there is some convergence internationally about the issues and techniques needed to address issues around privacy and information. They are universally international issues. There is a movement in that direction, but it is taking time to get that up and running.

> ***Dr Elliot***: Can I pick up the point on terms and conditions? There is an issue here. Even if you made your terms and conditions only 500 words, I still do not think people are going to read them, partly because of the language they are written in and partly because nobody has the time to do that sort of stuff. They want to get to the good stuff, as you said. I do think we need to look at technical solutions to this. There is existing technology with text mining and so forth by which you could have an app that distilled some of these terms and conditions and mapped them on to your own preferences. That is another issue here. Each user will have their own preferences about what they are and are not willing to do, and what they are and are not willing to allow a user of their data to do, and so forth. We also need to look at technical solutions to this.

Q181 Stephen Metcalfe: What about graphic solutions and icons you become familiar with that say, "Your data will be used in this way"? They can often speak thousands of words. Is there anyone doing that?

> ***Dr Elliot***: Companies?

Q182 Stephen Metcalfe: No, not necessarily companies at this point. I am referring to someone coming up with the concept of using icons or graphics.

> ***Dr Elliot***: We are now putting together a research project looking at exactly this. What would work for users in terms of representations of privacy content within terms and conditions? We are looking at traffic light-type systems and different ways of representing visually a particular pathway for your data and where it is going to end up, who is going to be using it and what the risks are.

> ***Dr Macnish***: At a more localised level, I believe Facebook is doing something along those lines with every status that is now posted. Whenever a status update on Facebook is posted, a question comes up as to whether you wish it to be public, to go out to friends or be private. I think that is icon-related as well, so work is being done at a very localised level rather than on terms and conditions.

> ***Steve Wood***: There is a need for standardisation to make sure we do not have the proliferation of too many different icons. A number of people have used the analogy of

nutrition labels, or labels showing the fat content of foods, but this area is a little more complex than that. It is not to say it is impossible, but we need to work collaboratively across a number of different areas to get those standards agreed.

The other area we are exploring at the Information Commissioner's Office at the moment is the concept of a privacy seal scheme. That would be a standard scheme we might be able to endorse, but we are still exploring that at the moment.

Q183 Graham Stringer: Mr Wood, you said you were in favour of privacy impact assessments. What would one look like?

Steve Wood: Essentially, a privacy impact assessment is a process that an organisation would work through, thinking about the information and data they have, making sure they understand it and how they may want to use it, or data they may want to combine in or add to that data, and specifically focusing on the usage of that data, the information flows and the impact on individuals and the various different scenarios that can unfurl from the use of that data. It is very much thinking through different options and ways to mitigate the privacy risks which are identified. There could be a number of different issues. Do we need to provide more information to users? What about security? It also allows an organisation to think about the issues before they start the process, which we think is very important.

We also hope that it introduces the idea of proportionality. There can be different routes that perhaps use fewer data to get to a result that still helps the organisation. Sometimes people see the prize, or think, “We can get to this result only by using this amount of data,” without thinking about whether there are different ways to do it. Can we use different forms of data? Would anonymised data, rather than fully identifiable data, help us in certain situations in terms of working through all those different risks and issues? The end product of a privacy impact assessment is ultimately a report which can propose different ways forward and different options, but the key point is that the issues are mitigated at an early stage. It is a process we have been promoting for about eight years at the ICO.

Q184 Graham Stringer: Should users be made aware of who owns the sites? These sites change hands, as you have pointed out. There can be fairly innocuous ownership and it can then end up in the hands of credit rating agencies. Do you think people should be automatically made aware of who owns those sites?

Steve Wood: Transparency is a key component of data protection legislation. It is very important that it is transparent to the user who is processing their personal data. Whether it is the ownership of the site, who is ultimately the data controller is a really important point. That has to be transparent to the user.

Q185 Graham Stringer: You say that as though it is at the moment, but it is not at the moment, is it?

Steve Wood: We can still find instances where transparency can be better and clearer. In particular, people's understanding of how credit reference agencies work is an area we recognise, and maybe we will be doing more work on that in the coming year.

Q186 Pamela Nash: Gentlemen, in what way can data from social media be used by Governments, first, in disaster response?

Dr Macnish: I think in locating and hearing about disasters much faster than the media can get hold of them, and hearing updates of what is going on. People are regularly tweeting about them. When the Egyptian revolution kicked off in Tahrir square the hashtag "#Jan25" was being used and updated so regularly that I was trying to keep up with it at the time. I remember that it was scrolling past so quickly I could not even read the tweets coming up on the screen. A tremendous amount of information can come out which can then be of use to the emergency services in those cases.

Q187 Pamela Nash: That is a good example. With information coming so quickly, do you think it can be utilised well by Government?

Dr Macnish: Absolutely. I think you can run algorithms against it even when it is coming through quickly. Obviously one person sitting down at a screen is going to struggle, but you can run it through an algorithm that would help to pull out defining trends that could then balance claims against counterclaims to see whether or not something is really happening. A fair amount of analysis needs to happen, depending on how fine-grained you want to get with the information you are receiving, but certainly there are benefits to be had from it.

Q188 Pamela Nash: Do we have the capability at the moment to be able to analyse that information very quickly and utilise it?

Dr Macnish: I could not say for certain. I am not a computer scientist. My understanding is that we probably do, but I do not know quite the volumes that we would be talking about as to whether or not we could deal with it. Each algorithm will have a certain parameter within which it can cope.

Dr Elliot: If the question is whether it would be possible, then, yes. This is just technology. For the disasters we are talking about, it is something instant like Twitter rather than more reflective social media. You are then just sticking data science on to the fire hose that Twitter produces. There is a whole issue about getting access to that. If you want to be able to respond in real time using that, some data science needs to be done; it is not just on tap. Work would need to be done if that is what you wanted. Infrastructure and probably some research would be needed in order to fit it to what purpose you had in mind. The first question would be: what would you want to do with it?

Dr Macnish: There would also be the follow-up. It could also be used as a communications channel from the emergency services to the people in that particular area, saying, "This is the hashtag, Facebook site, or whatever, that you should be following." This has been used to an extent in the States with the amber alert system, which seems to be quite effective. If there is a missing person, it goes out on Facebook. People get SMSs. It is a very simple form of communication that people sign up to, and then they can hear directly from the emergency services.

Q189 Pamela Nash: I want to look at national interests and how we use social media and the data from it to prevent terrorism and terrorist attacks. How can we use data to prevent these attacks, and how effective do you think we are at using those data at the moment?

Dr Macnish: I could not comment on how effective we are in using the data at the moment. There is potential for the data to be used. My understanding is that social media platforms are being used to recruit terrorists. There is going to be an increasing scale of involvement in terrorism, which might well be reflected in social media platforms. Communities and who you are friends with, who you connect with and who you follow might start to give indications. My concern is that we may end up in a dragnet scenario whereby all social media is collected and trawled through in a fishing trip expedition just to find the interesting information and to find the terrorists out of that. Going back to an earlier comment, just because the intention is good does not necessarily mean that, therefore, the consequences will also be good.

Q190 Pamela Nash: What would be the negative consequence of that?

Dr Macnish: I think Government having unrestricted access to citizens' social media would not be a healthy thing. You can find people's private opinions; people would feel extremely vulnerable. Privacy is a core element of a liberal democracy, and it would be unhealthy for the Government to have that level of access to people's information as a regular thing. If you find somebody whom you have good reason to suspect is involved or engaged in terrorism in some way, by all means with a warrant go after their information and take it, but the idea of having everybody's information collected just so it can be trawled through looking for trends is a worrying one.

Q191 Pamela Nash: Dr Macnish, can I take it that you are not a fan of the USA Patriot Act in that case?

Dr Macnish: No. I have two problems with the Patriot Act, both revolving around section 215, which is the most controversial aspect. One is that there appears to have been, from my limited understanding, a secret interpretation of that particular section, which I see as being wholly undemocratic. When Government take a secret interpretation of a law, it becomes very problematic. There is no sense of accountability of the Executive. The second thing is precisely what I said. It allows for dragnet collection. In the case of the States, that led to communications data from Verizon and other mobile phone companies going straight to US intelligence and being stored there. My understanding is that that has now changed in the light of the Snowden revelations, and those data are now held by the telephone companies and they can be accessed by the intelligence services when they have reason to suspect a particular individual. My understanding is that this latter approach is how the UK currently operates. That seems to be a much safer approach. The intelligence services require grounds to approach the telephone companies, internet service providers, or whoever it may be, to get the information they need on particular individuals and not on groups in general.

Q192 Pamela Nash: Can I ask your colleagues whether they have any comments?

Dr Elliot: I think you are only ever going to catch a stupid terrorist using social media. Any sensible terrorist is going to be using the dark web to communicate and network. It is the bad terrorists or the not very clever terrorists that you are going to get in this way. As to whether that is worth any significant use of resources, never mind the ethical issues my colleague has raised, I am very dubious.

Q193 Pamela Nash: I am just playing devil's advocate here. I take your point about a stupid terrorist, but the information that we are looking for is not necessarily someone putting details of an attack on social media. It might be a very nuanced analysis of trends that people are looking at, who they are communicating with and where they are travelling. That might mean a more extended look; it might be a wider range of people whose information is being looked at. Is that not something that you think—

Dr Elliot: I am sorry. I missed the nuance.

Q194 Pamela Nash: Dr Macnish made the point that it should relate only to people who are already suspects. If you are looking at information, it might be more difficult to ascertain, and a wider pattern is being looked at. It might be a wider range of people.

Dr Elliot: Is this like the "crimes about to be committed" type of analysis, which I have heard about?

Pamela Nash: Yes.

Dr Elliot: Perhaps you are saying, "Hang on. There might be something about to happen here." I think we are again in very murky water ethically. I understand there is some value in this technology, having spoken just yesterday to somebody from Europol. They are achieving some wins with that. Whether that should be done routinely and the resource required justifies the benefits is less clear to me.

Dr Macnish: To follow that up, the concern I have there is that the sort of pattern recognition you are talking about, looking for patterns that indicate somebody may well be involved in terrorism or may be about to engage in a terrorist act, is based wholly on statistical correlations. There is an 80% chance that somebody might be involved in terrorism, or something along those lines. Does that 80% chance count as grounds to intrude and monitor their telephone and communications? I don't know, but it just feels very uncomfortable to me that a statistical correlation would be sufficient. In a way, we almost deal with that already with profiling, saying that because there is a statistical correlation you should not just stop and search somebody. You need to have grounds for suspicion in that particular case. I think the same would be true here as well.

Q195 Pamela Nash: You have both touched on public perception and what the British public might think of different levels of Government use of social media data to protect national security. Mr Wood, what do you say is the general public view—not necessarily your own view—about how comfortable they are with the Government using their social media private data for national security purposes?

> ***Steve Wood***: A mix of views comes forward from the public. I think they have perhaps some understanding that their data, which may be old, may be used in certain ways, sometimes linked to national security or law enforcement areas. They do not have a full understanding of what happens. Sometimes they think more is done with their data in certain circumstances when it is not; in other scenarios, it is the opposite. We probably lack the public debate and true understanding and transparency about the extent to which their social media data could be used. Post-Snowden, what we probably have lacked in the UK is a full debate about these issues. The debate has been much more rigorous in the US. A good starting point for the debate is what further steps we can take to improve transparency and get people to understand the different ways in which particularly social media data can be used. That ranges from the things you have just discussed to perhaps more general uses relating to trends, and correlating and understanding issues. This might be in a very broad geographic area, which may have fewer privacy issues, compared with where you start to target an individual, or you probably need to consider issues about proportionality and what the effect on the individuals may be as well. I think we lack that debate at the moment.

Pamela Nash: To me, it is not a big jump from Tesco analysing whether or not a woman is pregnant by her shopping, and what vouchers to send her, to looking at national security issues, but that is a matter for public debate.

Chair: Gentlemen, thank you very much for helpful evidence and your written information as well. We may follow up some of these questions in a little more detail in writing, if we may. You have raised some challenging issues to which we would not do justice if we touched on them now. Thank you very much indeed for your time.

Examination of Witness

Witness: **Ed Vaizey MP,** Parliamentary Under-Secretary of State for Culture, Communications and Creative Industries, Department for Culture, Media and Sport, gave evidence.

Q196 Chair: Minister, thank you very much for coming in. We know that in all of your responsibilities you take a keen interest both in the Internet Governance Forum and, specifically here, the social media space. In your role as the responsible Minister, how much of your work is to do with supporting UK-based companies versus managing issues around US companies operating in the UK?

> ***Mr Vaizey***: It would be hard to divide that up. As Minister for the creative industries, I am a big supporter of UK businesses, and we help them in terms of their export strategy. If you are talking about the internet, it is pretty clear that, in terms of some of the issues that cross my desk, companies like Google, Facebook and Twitter are relevant. On the other

side, the main internet service providers—BT, a British company, Virgin Media, which is now effectively an American company, Sky and TalkTalk—would play a big role as well. We work with the main ISPs very much on issues to do with child protection and child abuse imagery, but we work on that as well with the big American companies Twitter, Facebook and Google.

Q197 Chair: But you have very little power to regulate the activities of those big American companies that have played a significant part in some of the evidence we have heard in this inquiry. How do you go about addressing that challenge?

Mr Vaizey: You have put your finger on this, Mr Miller, in one sense. In a very wide sense, that is the challenge for policymakers, not just in the UK but in almost any country, because a lot of the organisations one deals with now have a global reach but are based outside one's jurisdiction. On almost any policy issue, because of technology, you face that challenge. Nuisance calls would be another example. Companies from abroad make nuisance calls. How do you deal with that?

Without wishing to put a hostage to fortune on the table, I have found dealing with them reasonably straightforward. It is a challenge for Government at what point it wants to lay down the law, if I can use the vernacular. For example, on the removal of child abuse images, the Prime Minister was very clear that it was his intention to do everything he could to eradicate those from the internet. In that respect Google came to the table and made some very far-reaching changes. That was because the Government were emphatic in their position. I am sure we will cover a range of matters in this evidence session, such as issues to do with the right to be forgotten and data protection. These are issues where the UK Government have a say. Funnily enough, potentially, we have a stronger say because we can play our part in influencing European policy, which obviously has a big impact on companies outside Europe.

Q198 Chair: Within the UK data capability strategy, where does social media data fit into that discussion, rather than big data in its generality? Is there a specific piece of work going on in terms of how social media data is handled?

Mr Vaizey: I have read the evidence this Committee has received. I know that some of the people giving evidence indicated that social media should be a separate element of Government policy, if you like—that big data is one of the eight great technologies, and perhaps social media should be a ninth great technology. A wry smile crossed my face. If you are giving evidence and you come from the world of research where you are looking for grants to look at social media, it would be very useful if it was the ninth great technology. I think that for practical reasons social media fits within the Government's approach to big data. It is obviously an important element of it.

Reading the evidence, I think we are justified in saying that we are at a very early stage both in how we use social media and understand it. The Government are certainly aware of its importance and keen to work with academics and researchers to explore the implications, but in my view clearly social media sits within big data.

Q199 Stephen Metcalfe: Some very large numbers are thrown around about the economic benefits of looking at this. Someone suggested £216 billion by 2017—whether that is per annum or cumulative I am not quite clear—supporting 58,000 jobs. Are those numbers ones you recognise? Have the Government made their own estimates of what this technology—this field—could be worth, in terms of both social media and just big data?

> ***Mr Vaizey***: I am not aware of any internal Government research on this. These are the CEBR figures, which is a respectable institute. We all know that estimates of this kind are estimates by definition. Whether it is £216 billion, £150 billion or £250 billion, I think we can all agree it is probably a big number and it will create potentially thousands of jobs. Big data is one of the eight great technologies. Some people describe data as the currency of the 21st century. It has been described as the oil of the 21st century. It is clearly going to be extremely important. It is important that Government are ahead of the game in terms of their research and engagement with industry and academia on it. It is important that we are seen as a country that is looking at big data and lead by example.
>
> In terms of Government making data available, I think our open data policy is very important as well. When we came into office we made the very conscious decision that we would do our best to make Government data available, because that can drive business creation and innovation.

Q200 Stephen Metcalfe: You said we need to be ahead of the game. Do you believe we are and we are not playing catch-up with countries like the US or Japan?

> ***Mr Vaizey***: I think we are ahead of the game. There are some stats which are not estimates. One statistic I have seen is that we are the fourth largest country in terms of high-performance computing. If you look at the kind of investment we are making, whether it is the £40 million to the Alan Turing Institute—I gather that flesh has been put on the bones of that this month by the Engineering and Physical Sciences Research Council, which is responsible for it—the £189 million we have put into high-performance computing, or the £50 million we have put into the connected digital economy catapult, a lot of money is going into this. I have seen comparisons with other countries. The United States will clearly be a world leader; Japan is another one; and some people say India is good on this as well. I think we stand good comparison with other European countries, and certainly with others around the world.

Q201 Stephen Metcalfe: You talked about the great investment that has been put into areas that would support this field. It is good that the Government have invested, but how do you measure the return on that investment? What are the tangible results from that? It is great that you have done the investment. What do we get back for it?

> ***Mr Vaizey***: That is a really good question. I don't have an answer to it. As an MP who has a huge amount of science in his constituency, I am very happy to receive that investment. There was £500 million in the Large Hadron Collider. I have never asked for any return on that investment. It creates a base layer of both physical capital, in terms of kit that is being built and used, and also human capital. You attract from all over the world the brightest minds who want to work. I am sure there are statistics out there that we can read out to show the return on investment in scientific research in the widest sense that would give

good, strong figures. David Willetts has been very successful in protecting the science budget. I think the reason he has been successful is that the Government recognise that effectively this is investing in the skills, businesses and applications of the future.

Q202 Stephen Metcalfe: What I am saying is that, if we are going to invest in big data and social media data, we need to know whether we are getting our fair share of the alleged £216 billion, and whether it is worth investing more. One of the economic challenges we face as a country is that we do not have a big enough medium-size business sector. Medium-size businesses normally start from small businesses. How are we going to make sure that small and really medium-size enterprises get access to this and are involved in what I think will be quite an innovative space so that they will be able to maximise the economic potential?

Mr Vaizey: We are doing quite a lot of work on that. David Willetts is leading a lot of this. He has set up a high-performance computing council, as it were. That is a way of taking the very big businesses and research institutes, which put a lot of investment into high-performance computing—it can include companies like Jaguar Land Rover, which put millions and millions of pounds into high-performance computing to do their very sophisticated design work—and looking at ways to make it available to small businesses. Clearly, that is incumbent on big scientific institutions. I mentioned the Large Hadron Collider because it happens to be in my constituency. They are very keen to make sure that small businesses have access. We have a lot of small high-tech companies, often spun out of universities, which are working on very high-end scientific research effectively but clearly do not have the resources to spend £50 million on the kind of kit they would need. They need access. That is the kind of work going on.

Q203 Chair: I think you have Diamond in your constituency; I don’t think you have the LHC. Your boundaries do not stretch to Geneva, do they, but we know what you mean?

Mr Vaizey: I am sorry—it is the Diamond synchrotron. I do not know why I talked about LHC. It was a senior moment. Perhaps I have a yearning to have the Large Hadron Collider in my constituency. Perhaps I can start my bid for the next Large Hadron Collider.

Q204 David Tredinnick: It is reported that there is a shortage of people who have the right combination of skills for media and real time analytics. Do you think that is right?

Mr Vaizey: I am sure there is a shortage. With any emerging field, particularly one where the skill set is particularly niche, there would be a skill shortage. That would apply to Government and business. We are looking at skills across the board, from schools through to colleges, universities and, indeed, apprenticeships. Skills also affect our approach to immigration, so we want to ensure that the highest quality graduates are able to come and work for companies where they are needed.

Q205 David Tredinnick: To what extent do you differentiate the skills required for social media analysis and those required for other types of data?

Mr Vaizey: To answer that question intelligently would be beyond my level of expertise. I can write you a fuller answer to it.

Q206 David Tredinnick: Do you take account of those differences—I assume you must do—and to what extent?

Mr Vaizey: The Government will have their own programmes on social media analytics in wanting to understand how to use social media, in particular, as Ms Nash referred earlier, in terms of disaster and crisis situations. A lot of what we will be doing at the moment is working with private business as well. A lot of the call-outs from Government will be to work with the private sector, simply because at this stage, without being pejorative, it would be difficult to find people who join the civil service with a specific career path to do data analytics and social media analytics. We are in the early stages. We will use public private partnerships, like the connected digital economy catapult, to look at opportunities to do more work in social media analytics, and we will use the research councils, the Alan Turing Institute and so on. Working with universities, academia and the private sector would be the main way forward.

Q207 David Tredinnick: You touched on immigration. How do the Government plan to make sure that immigration policies do not adversely affect the ability to attract talent in social media analysis from abroad?

Mr Vaizey: It is important that we have a strong immigration policy, in the sense of wanting to ensure that there is control of immigration. At the same time, we are keen to ensure that we get people with the right skills into the country. We have a points system to ensure that we can get people with skills. There are two routes. Tier 2 (general) is for skilled workers who have a job offer and a degree. There are inter-company transfers as well. We also have a shortage occupation list so we can recruit people where we think there is a shortage of skilled workers. We also have special visas for academics. We have a fairly open market for international students as well. There is a range of different ways that we can attract the right kind of people to come to the country to help, in terms of both pure research and growing businesses based in the UK.

Q208 David Tredinnick: That is very helpful. I think we accept that we have an engineering shortage in the UK. What are you doing to try to help produce home-grown talent in the engineering sector?

Mr Vaizey: The Government have, first, a strong focus on engineering in schools. With my Minister for Culture hat on, I am often criticised that the Government are perhaps focusing too much on STEM subjects—science, technology, engineering and mathematics—but I think that is because of the recognition of the shortage. I was delighted when the Secretary of State for Education said that computer science should be part of the national curriculum. For many years people have complained to me that kids at school were learning how to use applications but not how to write them. That is a very ambitious move and it puts us ahead of the game. The challenge will be in the implementation and making sure we can get the right teachers in to teach computer science, but it is a big signal that we take it seriously.

Apprenticeships also play a valuable role in this. As you know, the Government now have a big focus on apprenticeships. I am hoping to get certain things in my constituency correct this time. For example, in Harwell the UKAEA has a very good apprenticeship programme. I think there are now lots of people who can get the engineering skills they need through the apprenticeship programme as well as through straightforward university degrees. To get students studying these important subjects is a perennial problem, but the Government are very aware of it and are focused on providing solutions.

Q209 Graham Stringer: The terms and conditions of online companies are often pretty impenetrable. What are you doing to monitor that situation? Do you think Government have a role to make those terms and conditions more comprehensible?

Mr Vaizey: I think you heard evidence in another session from Nigel Shadbolt and another member of the Information Economy Council, which is chaired by David Willetts and which I attend. We had a meeting yesterday to talk about the approach to transparency on data that you discussed with them in your evidence session, and a first stab was put forward. That led to an interesting discussion about the role of Government. Some people feel, funnily enough, that it is better—"wrong" is not the appropriate word—that the initiative comes from business and industry rather than Government. Being a politician, I find that quite hard to get my head round.

I think we have an opportunity; I want to move forward on this and I think we should move forward on this. My understanding is that the Information Commissioner's Office is going to be the conduit for this kind of work, with the industry coming forward with proposals to simplify terms and conditions online.

I think—the Committee probably shares this view—that the idea that people read 150 pages of terms and conditions is simply laughable; it is a complete nonsense. We all know what lawyers are like—every t is crossed and every i is dotted. But the consumer needs something that is easy to understand and straightforward.

Q210 Graham Stringer: I certainly think we are all agreed on that. What I am trying to get at—I am not sure from what you have said—is whether you have asked the Information Commissioner to carry out that work or the Government themselves are monitoring the situation. I think the problem is universally recognised, and I want to find out where the Government are on it.

Mr Vaizey: My understanding is that the work of the Information Economy Council, at which the initial draft was discussed yesterday, is going to be taking it forward, with the Information Commissioner standing behind that work and engaging industry to come up with proposals for simplified terms and conditions and a kitemark, which I think industry wants as well.

Q211 Graham Stringer: Will part of that review, assessment, whatever you would call it, be questioning the justification online companies have for asking for the information they seek, or will that be a step too far?

Mr Vaizey: I would have to give you my personal view, in the sense that the relationship is between the company and consumer. For me, I think Government's role is to ensure that the consumer understands that the company is asking permission, which is the right word to use, from the consumer to use their data in a certain way. We should not necessarily restrict what they want to ask the consumer about how they use their data. I think that ends up being too top down and potentially restricts innovation. Government's role should be to ensure that the consumer understands what the company is asking for and gives consent to that.

Q212 Graham Stringer: The Information Commissioner has alerted this Committee—I guess he has alerted the Government as well—to the fact that a credit reference agency has been buying social media sites. Are the Government concerned about that? Do they see a privacy issue there, or do they believe action should be taken when ownership changes so that the users of those sites know who the owner is and that it might be used for different purposes from those they originally envisaged?

Mr Vaizey: I am not the Minister responsible for the Information Commissioner. The Information Commissioner sits within the Ministry of Justice. My instinct is that the Government would want advice from the Information Commissioner about whether this was an appropriate thing for credit agencies to be doing. There has been debate in the Committee and elsewhere about people posting online in a public forum like Twitter. I think that technically it is still their data, but they have made it public. My understanding—I will correct it if I have got it wrong—is that that is now public data and, therefore, it is not a breach of the Data Protection Act to use it. Clearly, there are big issues involved here. There is the issue of what one does with data that are public, as in you have stated something in public, and what one does with aggregated data, which I think it is important should be kept anonymous.

Q213 Stephen Mosley: You will be aware that under the Data Protection Act a breach of section 55, which is unlawfully obtaining disclosure of personal information, is currently an offence but is backed up only by a fine. It is not a criminal offence and there is no prison sentence attached to that. Do you think it should be?

Mr Vaizey: I don't want to dodge your question, Mr Mosley, but I think that, emphatically, has to be a matter for the Ministry of Justice. If a Minister in the Department for Culture, Media and Sport decided to change the Data Protection Act—

Q214 Stephen Mosley: What would be your advice to the Ministry of Justice?

Mr Vaizey: It is not something I have turned my mind to.

Q215 Stephen Mosley: The Information Commissioner has told us that once data have been anonymised they lose protection rights, but there is a potential for those data to be reconstructed and re-identified. Should re-identified data have the same rights as unanonymised data?

Mr Vaizey: My understanding is that there is a difference between somebody in a position of public trust being able to take data that have been anonymised and reconstituted—that would be a breach of the Data Protection Act—and somebody sitting at home taking reams of data and trying to reconstitute it. My understanding is that that is not an offence. I can see the difference between that case and somebody in a position of trust who is using tools perhaps not available to the general public to try to identify an individual from anonymised data. I think that should be an offence, but going further than that would be to stretch beyond my own personal ministerial responsibilities.

Q216 Stephen Mosley: It is a very wide topic and we are aware that it covers a huge range of ministerial responsibilities, but I do want to press you on this a bit. Do you think that the re-identification of anonymised data by someone not connected to a public body should be a criminal act?

Mr Vaizey: I am not aware that the Government take that view, and it is not my view at present.

Q217 Mr Heath: Minister, do you deal with the European Union data protection regulations and the proposed new ones?

Mr Vaizey: Not at all, but I am happy to answer questions.

Q218 Mr Heath: You are familiar with the Government's response.

Mr Vaizey: Yes. Funnily enough, I always bump into Chris Grayling at the airport when he has had a discussion with the commissioner in Brussels, Viviane Reding.

Q219 Mr Heath: On that basis, the Government's position, as I understand it, is that they are not particularly keen on the proposals coming forward. One of the areas where they are not keen is the issue of explicit consent. We heard earlier that 80% of the British public are concerned about the way their data are potentially open to misuse. What is wrong with explicit consent in your view as a mechanism?

Mr Vaizey: The issue is this. What we want to achieve in Government is a balance with the rights of the consumer. Perhaps I should not say "a balance." The rights of the consumer are paramount, but one has to be pragmatic as well and not inadvertently stifle innovation. One issue that I did work on very closely, because it fell within my remit, was the e-privacy directive, which was a similar piece of legislation coming from Europe. It was about how you inform users of websites that cookies can effectively track their browsing history. Some would say that can be of benefit to consumers because they are served up with adverts that are relevant to their interests.

We worked closely with business to ensure that its implementation did not introduce too heavy burdens. If you go on a website, you will now see in a pretty straightforward fashion a banner saying, "We use cookies. Click here to find out more about them." Similarly, the advertising industry, of its own volition, has come up with AdSense. You can click on an advert and they will tell you why you are seeing it and show you some background as to how it works. I think it has been successful.

We also work very closely with the Information Commissioner. He made it very clear that he would not prosecute people in the first year. He would allow them to try things out and come to him and explain why they were doing it, and he would provide feedback to them and say, "Well, you're doing it slightly wrong in our view."

Explicit consent can lead to excessive bureaucracy. It can also damage the consumer's experience, which was the debate we had about e-privacy, if they have to keep giving consent at every stage of their interaction with a business.

Our other concern about explicit consent is that it ends up trivialising consent. Explicit consent sounds and is a pretty important decision made by the consumer. If for every single transaction with a business that involves giving them data you have to give specific consent, in a sense, if everything is explicit consent, nothing is explicit consent. Consumers will then start giving explicit consent as a matter of course, because they want to get on with the transaction they want to have. That is why we are concerned.

Consent is important to the consumer. It is their data; they have the ultimate right, but it is also important to be pragmatic, funnily enough, on behalf of the consumer, who also wants a relatively seamless transactional relationship with the business they are interacting with.

Q220 Mr Heath: I understand that, so what is the alternative? How do you give uninformed consent without being asked regularly to do so?

Mr Vaizey: You can provide informed consent by giving it, as it were, at the beginning of a transaction and your relationship with a business, whether it is a supermarket loyalty card or a website where you regularly shop. You can give specific or implied consent by getting a clear explanation, perhaps with reference to the discussion we had earlier, of the broad terms and conditions to which you are signing up, or the broad ways in which your data are going to be used, so that from then on your relationship can continue.

Q221 Mr Heath: You would favour a generic consent: for example, "I give my consent to this sort of use of my information."

Mr Vaizey: Yes.

Q222 Mr Heath: How about Government use of that information? Should that be one of the boxes you tick or do not tick?

Mr Vaizey: I think Government have to be beyond reproach when it comes to their relationship with consumers. They have to ensure that, when you are transacting with Government, particularly as we are moving into a digital relationship with a lot of citizens, that is included. With reference to my earlier answer, if a company wants to say to you, "Mr Heath, please give us your consent, and we may give your data to the Government," it is for the company to say that to the consumer, so long as the consumer knows—

Q223 Mr Heath: Would that include national security?

> ***Mr Vaizey***: Potentially. I am not an expert on national security, but clearly it could include a reference to the fact that the Government may be able to access your data for national security reasons.

Q224 Chair: You may have heard an earlier witness argue that there ought to be a process of, almost, applying for a warrant to access my data. Do you think there is merit in thinking about that more deeply?

> ***Mr Vaizey***: A warrant from Government?

Q225 Chair: In the same way that a police officer seeking to search your house would require a magistrate's warrant. Do you think there is a parallel in the virtual world that could strengthen public confidence in relation to Government potentially abusing their datasets?

> ***Mr Vaizey***: The Government set out clear policies on how they will use their national security powers to access data. Those powers are subject to judicial oversight and are clear, but I would not wish to second-guess my colleagues in the Home Office about the right way to protect people.

Q226 Chair: I come back to your point about explicit consent being a difficulty because it is intrusive. If it is intrusive, you have to ask yourself why companies are asking for so much information. Shouldn't companies be encouraged to seek less information? We had an example the other day where a colleague was downloading an app and the system wanted to know his location. It was totally irrelevant and it was an unnecessarily intrusive request for information. Shouldn't that kind of thing be actively discouraged by Government?

> ***Mr Vaizey***: I do not know whether it should be actively discouraged by Government. I certainly think there should be a debate about the amount of information a company may wish to get from you. If it is asking for a location service for a music app, where you are listening to the music may well be irrelevant.
>
> What I want to say, Mr Chair, is this. It is easy to forget, perhaps not for those of us who are approaching or are past middle age, like me, that this industry to a certain extent is in its infancy. It is a bizarre position to be in that the two largest companies in the world are effectively younger than all of us.
>
> My hunch is that, in terms of the reams of terms and conditions that apply to a lot of these sites, that is the lawyers at work—presumably, they are getting hefty fees for covering every eventuality—plus the start-ups and innovators with their new applications, who are thinking, "We want lots of information because that might drive the next iteration of the business and the business model." Presumably, your colleague who found the location data intrusive was given the option to provide it or not provide it. The people behind that app might think that in a year or two having that location data could take them to the next stage of how the app is used.

Q227 Chair: I return finally to Government, and I appreciate this is a question that goes well beyond your own remit. So just answer in terms of your own remit, which spills over. You have relationships in DCMS with health in relation to sport, for example, business, criminal justice and so on. A very complex crossover brief exists in your Department, so you must have some inkling as to whether or not the current approach to data sharing within Government remains—as one witness said—a challenge. Do you think we have cracked it yet?

Mr Vaizey: No, I don’t think we have cracked it; it is a challenge. Government need to do much more about data sharing. Across the piece in Government, single Departments make it very hard to do cross-departmental working. We have made great strides with the Government Digital Service. The work they have done has, in my view, been truly ground-breaking in crunching together thousands of websites into one site. What that is going to do in terms of data sharing is allow Government to have an overview of how the citizen transacts with Government. From that will emerge information that will help different Departments link up in terms of how they provide services for citizens, and hopefully we will see more sharing, more effective services and so on. That can link up health data, pensions data and so on.

Individual Government Departments are forging ahead in how they are using social media and also data. Some are better than others. The Department for Environment is lauded as one of the most effective in terms of using social media both to anticipate potential issues coming up but also to deal with them. Other Government Departments, such as the Department for Transport, in sharing open data are very innovative in how they have made it available. But, yes, we are also at an early stage. I would encourage the Committee to look at the work of the Government Digital Service. I think that is the pioneer. It is part of Government, but it has the air of something that sits slightly outside it, which allows it to be a relatively rare thing in Government—to be truly quite innovative and act almost as a start-up, which I happen to think is a positive thing; others might think it is a negative thing.

Chair: Minister, thank you very much for your time this morning.