



HOUSES OF PARLIAMENT

Joint Committee on Human Rights

Oral evidence: [The Right to Privacy \(Article 8\) and the Digital Revolution](#), HC 1810

Wednesday 3 July 2019

3.15 pm

[Watch the meeting](#)

Members present: Ms Harriet Harman (Chair); Lord Brabazon of Tara; Fiona Bruce; Ms Karen Buck; Joanna Cherry; Baroness Hamwee; Jeremy Lefroy; Scott Mann; Lord Trimble; Lord Woolf.

Questions 9–18

Witnesses

I: Dr Reuben Binns, Researcher, Department of Computer Science, University of Oxford; Professor Victoria Nash, Deputy Director, Associate Professor, and Senior Policy Fellow, Oxford Internet Institute, University of Oxford; Madhumita Murgia, European Technology Correspondent, *Financial Times*; Jed Mole, Vice-President, Marketing, Acxiom; Alex Hazell, Head of UK Legal, Acxiom.

Examination of Witnesses

Dr Reuben Binns, Professor Victoria Nash, Madhumita Murgia, Jed Mole and Alex Hazell.

Q9 Chair: Welcome, everybody, to this meeting of the Joint Committee on Human Rights. We are half Members of the House of Lords and half Members of the House of Commons. As our name suggests, we are concerned about human rights. The subject of this inquiry is the human right of privacy in the digital age. We are very grateful to you for coming to give evidence to us.

The windows are open to stop us all getting too hot, and because there is a bit of noise outside the microphones do not seem to be keeping up very well, so do you mind speaking incredibly loudly to us, in an unnatural voice, and not using initials? We would rather know something that you spell out to us laboriously than miss it, so help us into your area of expertise but without loads of initials and shorthand.

Thank you very much indeed for coming to give evidence to us. Could I ask you very briefly to give us your name, in a loud voice, and say what



HOUSES OF PARLIAMENT

your sphere of work is? Then I will pose the first question.

Alex Hazell: My title is head of legal for a marketing data company called Acxiom Corp and I am focused on Acxiom's UK businesses.

Jed Mole: I am head of marketing for Acxiom, the same company that Alex works for.

Madhumita Murgia: I am a technology journalist at the *Financial Times*.

Professor Victoria Nash: I am deputy director at the Oxford Internet Institute at the University of Oxford, where we study the societal implications of digital technology.

Dr Reuben Binns: I am a researcher at the department of computer science at the University of Oxford and a research fellow at the Information Commissioner's Office. I research privacy, data protection, and the web and smartphone app space.

Q10 **Chair:** Thanks very much indeed. Feel free to comment on, add to or contradict each other's answers, or to give a different perspective. We are very grateful to you all for agreeing to come as a panel together.

Can I ask the first question? There are rules about data collection that are designed to protect our right to privacy. Are companies complying with the rules governing data collection? Can you give us any examples of where data collection by private companies has had far-reaching consequences on people's lives?

Are there any specific trends or practices that should particularly worry us as individuals? Most people are in a state of acute relaxation because they have no idea what is actually going on, but are we right to be in a state of acute relaxation, do you have examples of any trends and practices, and are the rules complied with?

Madhumita Murgia: One specific practice that we should currently be worried about, and which is on lots of people's minds, is online advertising. There is an entire market and ecosystem of companies that serve us advertising on the internet. This is being looked at by the ICO—the Information Commissioner's Office, where Reuben works, and other authorities in the UK, which are concerned that the way our personal data is being used is not legal and infringes upon everybody's privacy.

Specifically, there is an auction system in the way online advertising works. Think of it as an online auction where the people who want to put the ads in front of you are bidding for your eyeballs. If I am on one side, as a user of the internet going to visit a website, there are hundreds of companies that might want to advertise their product to a 30-year-old woman who lives in London, works in media and likes to buy clothes, for example. The system is set up so that, when you visit this website, a profile about who you are is sent out and people are asked to bid. Companies then decide if they want to place their ad in front of you and



HOUSES OF PARLIAMENT

put out different bids. There is one winning bid, and that is the advert you see in front of you on your page.

If you think about how we use the internet, that has to happen in a matter of milliseconds, which is the time between you getting to a website, the page loading up and you seeing that advert. This cannot happen through human hands, because we cannot think and act in milliseconds. The entire set-up is called programmatic ad buying, because it is basically done by machines.

This is concerning, because nobody knows what is being done with their data. Let us start with what the data is. It is all sorts of data about our behaviour. It can be your IP address, which means your exact location; in some cases, your actual latitude and longitude are broadcast out. It can be where you live, where you work, what you like to buy, what health conditions you are interested in, where you are travelling to, everything you do in your daily life, what you have bought in the real world, political preferences or sexuality.

The concern is that special category data that are protected, including race, sexuality and your health status, are being broadcast out to companies. We have no idea whom it is going to. We have no idea what they are doing with it. There is no transparency, basically. Lots of people are really interested in understanding how it works, because it is very murky and opaque.

Chair: We are not giving our consent, when we go to a page, for this material about ourselves to be sold.

Madhumita Murgia: Technically, you are. That is the little pop-up that says, "Hi, we are putting a cookie on your device. Take care. If you agree to be profiled, in return you get to use the internet for free". That is the bargain we are making. The issue is that we do not know what happens to our data after that one company takes it. We do not know how many other companies are buying and selling the data and then using it to track you around the web.

Professor Victoria Nash: You explained that beautifully—well done. I would add a couple of things. Another aspect of where this departs from what might be seen as informed consent to existing data protection requirements is in the difference between the data you are consenting to give up and the inferences that can be made from it when it is put together.

One of the more worrying trends I see is the extent to which, as you said, every aspect of our lives these days is supported by computing devices. These generate vast amounts of data about us and we have very little way of ever telling how that data is used, the types of inference it generates or the effect those inferences will have on our lives. If their only effect is on what adverts I am served, I probably will not worry too much, but my understanding is that they may be used in many other



HOUSES OF PARLIAMENT

areas, for example to affect the price of goods you are offered and the array of products that are served to you. They may be used in terms of transfers to health and insurance companies, and the technologies we use at work. The way in which inferences are drawn from this wide array of data is a trend that worries me.

The second is slightly more fundamental. Maybe it goes too far beyond privacy for you to worry about, but it concerns the normalisation of what is effectively surveillance, which I hasten to add I engage in; I give up my data just as willingly as anybody else. But we are normalising these practices of surveillance, whether in our own online practices or, as in my case, even in parenting, for example. This is going to have much wider social implications, which we are perhaps only just starting to recognise.

Chair: Just explain the parenting point.

Professor Victoria Nash: One of the growth areas—particularly in the US, but it is starting in Europe—is baby tech, a wonderful sector that did not exist for most of us when we were first having our children. You can now get smart baby nappies, baby cots, baby monitors and baby socks, all of which collect data about a minor, who is below the age of digital consent, and use it to feed information into algorithms that help parents to decide, say, whether to change a baby's nappy, whether they are sleeping soundly or whether they have some signs of an illness.

In the example I am talking about, pre these technologies one would perhaps have used parental judgment and a relationship with the child. Increasingly, we are relying on a datafied relationship, based on what the technologies tell us, to make that sort of decision. As I said, it may be too far from your area of inquiry, but this is a broad social trend that I am concerned about.

Jed Mole: From an Acxiom point of view, fear is a powerful emotion. There is an important trend that we need to address concerning the transparency and understanding of how data works. My colleagues here on the witness table have made very good points about areas that we need to understand better. It is about separating the things that are perhaps fairly benign from those that are more concerning. Unless we achieve that separation, we are going to fail to get good at data. We will not be able to turn data off; we all need it in our lives. We need to focus on the areas where data is used in more controversial or sensitive ways, or used illegally. We need to get good at dealing with that.

We need to understand that data can be used for very good things. It is used to help businesses know their customer. For ever and a day, it has been a good idea for businesses to know their customer, because individuals choose to live digitally, and rightly so. I know I do. Businesses now need to operate digitally to know their customers and offer relevant ads.



HOUSES OF PARLIAMENT

It is right to raise awareness and draw attention to these things so that we get good at dealing with them, but among the scaremongering and concern we need to understand that a lot of this is simply someone showing you an advert that is more relevant to you. If a car company thinks you are in the market to buy a car, it will look to show you, rather than someone who is not, its latest offer for its latest model. If you live in a high-rise building, people who sell garden equipment do not want to show you an advert, because not only is it a waste of your time but a waste of their resources. If they waste money on advertising, their costs go up, as does the price to the consumer. It is an incredibly complex equation.

Chair: In the scenario that has just been painted by Ms Murgia, could you tell us how your company fits in? At what point are you doing what?

Jed Mole: There are two parts to the Acxiom business. First, we help businesses to design and build their marketing databases and technology so that they can manage their data securely and use it for better marketing. In the smaller part of our business, we work with partners, with publicly available data, to create marketing data products. We work with brands, to help them understand their customers better, which means that if they want to engage in online advertising or social media marketing they stand a better chance of placing an advert that is relevant to the audience.

Chair: Where do you interconnect with the scenario that somebody opens a page to look at something and somebody then buys access to them? How do you fit into that?

Jed Mole: We have various relationships. Again, some of it is directly with the brand, and some of it is with advertising agencies and platforms, where we will process data. We can combine first-party data, which is the brand's own data—let us say a car company's data—with Acxiom data or other data, which is termed third-party data.

It happens in different ways, to be honest. It can be complex. Sometimes it happens beforehand and is loaded up, for example, in case someone who fits the audience comes online. With the platform, the insights are applied when the person hits the page.

Alex Hazell: There is a basic distinction between the data that Acxiom uses and the remainder of the ad tech world. In the so-called ad tech world, data is passively collected across devices using cookie technology, and technical consent is given via cookie banners, which are getting more and more pronounced.

There is a question about the extent to which in the real world that is meaningful consent, even if it is technical consent. The passively collected data that the ad tech system works with is gathered through this cookie technology, which extracts information from people's browsers and then produces profiles.



HOUSES OF PARLIAMENT

In contrast, the data Acxiom works with is actively volunteered. People go to a competition website, enter a competition and actively volunteer their data. They type their data into a web browser, in contrast to this passively collected stuff, which is done through cookies. That is the key distinction between the role Acxiom plays and the remainder of the ad tech ecosystem.

I know you had a session on consent. The challenge for the ad tech world in relation to consent is that unlike under the data protection rules, where you have six legal grounds upon which you can process data, in the ad tech world there is only one ground to use cookies, which is consent. It is the only game in town. That is why ad tech companies using cookies cannot rely on the other grounds.

Goodness knows what is going to happen after Halloween, but from my perspective there is an opportunity to revisit this point and reflect on whether there is a better, alternative ground against which non-essential, low-intrusion cookies can be used lawfully. Some of the alternative grounds under the data protection rules could be used in relation to the non-essential, low-intrusion cookies that we are talking about, which usually work in this pseudonymous world, so it is not actually Joe Bloggs; it is usually an online identifier. That is a change to the law that would assist the ad tech community in this country, possibly in the coming months.

Dr Reuben Binns: The descriptions of how this system works that were previously given were a great overview. It is worth emphasising that it is not just the users of these apps and websites who are not aware of what is going on in the intermediary complex web of ad technologies. Very often, the website developers, the publishers and the app makers are not aware of the full extent of the data they are allowing to be given away. If I am an app developer, I no longer write all the code that goes into my app. If I am making an app, I will include a lot of third-party code from companies such as LiveRamp, which I believe is a subsidiary of—

Jed Mole: It is not any more.

Dr Reuben Binns: It was a subsidiary of Acxiom. That means that when someone uses my app, code written by another company is part of the ad tech system, which usually sends an identifier, often an advertising identifier, to that company.

The developers of these apps are not necessarily fully aware of all the different parties that might receive that information. You may think you have a relationship of trust between a user and an app developer, when in fact the app developer may not be fully in control of everything that is happening within the app they have developed. The same thing applies to many websites. A great deal of third-party code is included in these websites, which facilitates the harvesting of data for advertising technology purposes.



HOUSES OF PARLIAMENT

My colleagues at the University of Oxford and I analysed a million smartphone apps and found that the average one contains third-party code from 10 different companies that facilitates this kind of tracking. Nine out of 10 of them sent data to Google. Four out of 10 of them sent data to Facebook. In the case of Facebook, many of them sent data automatically without the individual having the opportunity to say no to it.

There is a great deal of collection happening which the app developers are not aware of. The traditional advertisers and the brands that fund this technology might not be aware either of everything that is going on in the background, so there is a need for those operating in the middle to be more transparent about how they operate.

Chair: It sounds a bit like what happened with the global financial crisis, where for half the people inside the system there was no transparency across it. We all know where that ended up. Thank you very much for those answers.

Q11 Scott Mann: Can I break my questions down to Reuben, Madhumita and Victoria first? Data collection has been described as the new oil rush. Everyone is out there trying to get information. We as MPs and Peers are bound by GDPR. There seems to be a bit of a dichotomy here with, on one side, very tight regulation about how you can use information and then, on another side, what I would describe as the Wild West in terms of data collection.

Is there a difference between the consent to use your information agreed on a free website and on a website you are paying for content on anyway? Should organisations such as Facebook, because they are providing the platform for you to use a free service, be able to utilise the information you are giving and sell it to third parties?

Dr Reuben Binns: I can talk about what we found when we showed users the hidden data collection that goes on in the background and asked them what they thought about it. They looked at apps they had paid for or apps developed by organisations that did not need to turn a profit. They were quite shocked at the amount of information that was being shared beyond the app.

There is the famous saying that if you are not paying for the product, you are the product, but it is also true that even if you are paying for the product, you may still be the product, because these business models are multisided. In researching how users react to these different business models, we found that many of them are uncomfortable with that.

Professor Victoria Nash: From my perspective, for meaningful consent I would like to see a choice in all cases between, for example, a paid-for app and a free version of that app, where it is very clear what data you will have to give up to have access to the free app. Even that would not necessarily set my concerns to rest, because, for example, I would not want to see a two-tier internet, where those who can afford it pay for



HOUSES OF PARLIAMENT

apps and services knowing that they will then not be tracked, while those who cannot afford it have to give up their data in return. I recognise that there is a difference in practice, but there is not as much difference as you might expect. Even the trope of there being some fair exchange falls down, quite frankly.

Madhumita Murgia: There is a social contract between all of us and our use of the free internet. Yes, we get all these great social media, communication and expression platforms and services for free and, yes, we do not mind being advertised to, especially if that advertising is relevant and targeted. That is agreed, and people want to use the internet for free, so they are willing to give up some amount of data, but the problem here is that it is completely out of control. The amount and type of data collected has become increasingly invasive.

When I was investigating a story a few years ago, I looked at apps that women might use, such as pregnancy-tracking and period-tracking apps. The type of information being shared included due dates and your monthly cycle. I looked at WebMD, a medical website where you can look up symptoms. You search "I have symptoms for", and it could be HIV or a sexually transmitted disease. All of that is transmitted on to third-party advertisers.

The question is how much they really need to know about you to show you an advert for something you want to buy. It seems that the line for that is way back there, and companies are monetising and exploiting these profiles in a way that goes beyond giving you a service.

Scott Mann: To build on that, I have a smart watch in front of me. I have just taken it off because the battery in my phone is flat, but I have given my consent to that organisation for the use of that data. How many lines of deviation from the information they pull from that smart watch is an acceptable level of deviation? They know how often I am sleeping and the times I am sleeping. Do they use that information to sell me mattresses? How many lines are acceptable from me giving my consent for a company to use that information to monitor my heart rate?

Professor Victoria Nash: What do you mean by lines of deviation?

Scott Mann: I mean if they want to sell me a mattress because they know I am not sleeping very well.

Professor Victoria Nash: As other panel members mentioned earlier, this is a complex ecosystem. The problem is not so much the adverts I might be served as a result of having a smart watch, so long as I understand the huge array of data it is collecting, because a lot of people might not be aware that things like your sleeping patterns are useful data for a company that might sell you adverts. That is one difficulty.

As I said before, it is not always clear that this data is kept within advertising networks. Look at companies like Experian. I understand from the Big Brother Watch submission that Experian data is used in the



HOUSES OF PARLIAMENT

development of the police force's new technology in certain parts of the UK. The lines of deviation are getting further and further away from what you would expect the use of that technology to be. That is a worst-case example for me, and I would be enormously unhappy.

Madhumita Murgia: I want to add a couple of examples of non-advertising uses of personal data. This is the big takeaway. It is not just about an annoying ad following you around the internet. An investigation of job ads that were served on Facebook found that lots of companies, including Amazon, Facebook itself and Goldman Sachs, were gating at what age people should see those ads, essentially discriminating by saying, "We only want young, hip people to work at our company, so only show this advert to people between 20 and 40".

They interviewed older people and said, "Would you want to go for this job?" Of course they would, but they were never given the opportunity to see that advert. In an increasingly digital age, where do we look for job adverts? You are going to see them online, which is where you will go to look for them. If you are never even given the chance to see them, it is not a choice.

There is another Facebook example. They are not the only ones who do this, but it just so happened that this was looked at. They were accepting ads aimed at categories such as "Jew haters", housing ads that were discriminating by race and a bunch of other things, which they stopped doing, but it was possible for advertisers to target specifically on those measures.

Lenders are now using social media data to decide whether somebody should be able to get a loan based simply on things like their behaviour via social media. How trustworthy are you, based on photos you have posted or even what kind of phone you own? An Apple user tends to be wealthier than the average Android user, so is probably more likely to pay back a loan. It is not just about advertising; it is about making decisions about recruitment, lending, admissions and other things.

Q12 **Scott Mann:** This is a question that the public would like an answer to. With devices such as Amazon Alexa and Google Home, there is a general view that people are receiving adverts based on conversations they are having in their own homes. I would like to know whether you think that is happening, because there is a lot of information on the internet to suggest that it could be. If it is, where is the line of consent on such a product?

Dr Reuben Binns: I had a conversation this morning about this. It is very easy to assume that the adverts you see are inferred from conversations you have, but in many cases the inferences you think are drawn from conversation are due to the masses of data that they already have about you through other means.

If you are on holiday, there is a nice view, there is a bench with a table, and you think, "This would be a nice place to paint the scenery". You sit



HOUSES OF PARLIAMENT

down, you log on to the nearby wi-fi and then you get an advert for a painting set. You might think, "Wow, they know where I am and that I have had a conversation with someone about doing a painting". It might just be that the previous person who was sitting in the spot had the same idea and bought something. Therefore, the correlation between their purchasing behaviour and your position in space is what led to that targeting. In many cases, it is not that the device is listening to you.

However, there was a case in Spain recently. La Liga, the Spanish football league, has an app that you can download. It turned out that this app was listening through your phone's microphone to see if it could hear the sound of a football game that was being broadcast through La Liga. If that happened and you were in a business location that did not have a licence to show La Liga games, it would flag that to La Liga, which could investigate the business for showing a pirated version of a football game.

That was a case where the microphone was being used to listen to what was going on around you, but in many cases the inferences can be made without having to record you. Whether it is done through the microphone or through your behavioural data, that is what we need to worry about.

Professor Victoria Nash: In some ways, I find it even scarier that advertising technologies can almost beat me to the point at which I express a desire to do or have something, because they have access to the same set of environmental prompts that I do. I agree with Reuben that in some ways this may be less sinister than listening in, but it is still sinister.

Madhumita Murgia: The more that different types of data are collected, the more that types of data can be used in different ways to listen to you, to sell stuff or whatever. Now we interact primarily through screens with the internet, but as we start interacting through cameras, facial recognition and using our voice, that is all data about us that is being collected by corporations. That can and will be used for what could be benign or malign purposes, but the data is being created and stored and is owned by corporations. It is a question of what happens next and whether we want to safeguard it, not whether it will ever happen.

Q13 **Ms Karen Buck:** There was an argument a week or two ago about apps that allowed access to people's stored photos without people understanding that that was implicit in their use of the app. I wondered if you had a view on the extent to which algorithms have been known to draw upon the content of messages and photos, how that access is used and whether people understand the extent to which it is drawn on.

Dr Reuben Binns: I can talk about how permissions work on Android, which is the largest smartphone operating system. When you download an Android app, it will ask you to grant permissions for things that the app wants to access. One of those is photos. It could also be your contacts, so the phone numbers that you store in your phone. You can do that on a per-permission basis, so you grant access to location but not to



HOUSES OF PARLIAMENT

contacts. However, that does not distinguish between first party and third party—between the app itself, which might have a reason to access your photos, and third parties that want to access them for advertising purposes. That is one of the problems.

The other problem is that in many cases the permission model can be circumvented. A developer can include code that can infer information that it has not explicitly requested permission for. Those are two reasons why the permission model that we have at the moment for smartphone apps does not really work, and people are concerned about things like apps accessing their photos because it is not clear why an app would need access to your photos to give to another third party.

Ms Karen Buck: How will my information gleaned from photos or from message content be used by companies?

Dr Reuben Binns: It could be used to profile you, to figure out keywords that might be useful for advertisers—all the things mentioned before. You could imagine a landlord using a service to assess a tenant's suitability, insurance pricing, et cetera. In the same way in which our clicks and search terms can be used for these things, photos and other data can be analysed for those purposes.

Madhumita Murgia: The app mentioned in the previous session was the Ocado app, a supermarket app. Sometimes, as I said before, the amount of data collected is unnecessary, so they might not want to do anything with it, but it is the fact that they have access to it and all our photos might be on some server that has not been secured properly, leaving them open to hacking or to losing that data. Then it unexpectedly ends up in the hands of people who want to sell it or have other ideas of what to do with it, and Ocado is just the scapegoat there.

That is part of the reason why it is not a good idea to collect more data than you need, because then you are responsible for that data and for securing it, which is part of the data protection regulation. Lots of companies are thinking about why they need the data they are collecting, because it just takes more money to secure it.

Jed Mole: Following the last session and this mention of Ocado, I do not know if any of you did, but this morning I downloaded the Ocado app and signed up. I could find no evidence of it wanting to access my pictures or phone. I need to continue the research, but as far as I could tell it was not asking for any of the things that were mentioned in the last session.

What I really like about the comments so far is this: if we can separate the things we are troubled about from the things that seem relatively benign, that is the first big step we could take to get good at what we are trying to achieve here. Is the watch you are charging a Garmin Forerunner 235?

Scott Mann: Yes.



HOUSES OF PARLIAMENT

Jed Mole: This is just one example of how the internet can help us. That is not me invading your privacy; I will tell you why in a sec. When we talk about the free internet, it is very easy just to throw out that term. What do we really mean by that? How many of us have paid to use email, how many of us have paid for a Google search, how many of us have paid to use a map when we say, "I will meet you somewhere" and we just take our phones out and follow it? Then there is social media and more. It is very significant and part of our human rights to freedom of expression and of association. It also affects education and the right to play.

Let me give you one tiny example of how it can help. Just after Christmas a friend of mine said, "You need to get back into running", which I thought was kind. He said, "You need to get a running watch, because it will really help you", so I googled a Garmin Forerunner 235, the very watch that he recommended. Everywhere I could see it was retailing for £240 to £250. Would you say that is about right?

Scott Mann: Yes. That is what I paid.

Jed Mole: Within three hours, I had an email. That is called email retargeting. Basically, the browser recognises that you are looking for a certain product and makes relevant associations. It is not looking for me as an individual, but I got an offer for the watch from Amazon for £178. I saved £72 and I had to do nothing other than search.

A lot of people think that retargeting is scary because someone has been watching what they are doing, but they do not realise that it is usually anonymous pieces of code that are working in the background. They do not care who I am. They are not trying to figure out what I had for breakfast or anything like that. Basically, an advertiser has a great offer and I am looking for that great offer, and it puts the two things together. There are scary examples, but there are also some very simple and benign examples.

Scott Mann: How do you say the name of your business, by the way?

Jed Mole: Acxiom.

Scott Mann: You are quite right. As an example, there is a condition called dry eye, which is prevalent predominantly in Cornwall but in other places as well around the country. We do not why this condition happens in Cornwall. If we had the data on why it was so prevalent in Cornwall, we could probably work out why it was happening and solve the challenges with that particular issue. I accept that data has a place and that collections of information can improve people's health and well-being.

My question to you is: where is that ethical line? How much is too much consent?

Alex Hazell: To pick up that example, dry eye is a medical condition, so any data processed in relation to that condition would be special category



HOUSES OF PARLIAMENT

data. We would never do it. It is a red line that Acxiom would never cross, but if we took Acxiom's dataset, combined it with people with dry eye and tried to spot some trends, in my view that would cross a red line, because the Acxiom data would become what, under data protection rules, is called special category data, which the legislation treats as a particularly sensitive form of data. That includes health data.

As soon as you join what is used purely for marketing to a list of people with dry eye condition for profiling and spotting trends, that marketing information becomes special category data. We would not cross that line. It is an example of responsible, ethical data stewardship that Acxiom believes in. That is one line we would never cross.

Another term used in the data protection laws is that it is more difficult to justify processing if what you do produces legal or similar effects. Employment screening, screening out people from particular jobs, is an example of where the processing would produce either legal effects or similar effects. That is another red line that Acxiom does not cross.

I am trying to explain here that the existing data protection framework already has a lot of checks and balances in place that, if you follow, as Acxiom does, you remove many of what I call the edge cases, because the vast majority of the marketing and advertising industry is trying to do the right thing. It is certainly not perfect, and there are many reasons for that. There need to be improvements, but if you follow the ethical considerations that are already built into the framework, you are putting yourselves in a good place.

We should focus on harm. If you remove these edge cases, what is the harm of receiving an advert that is more relevant than random? What are we trying to guard against? We should take a risk-based approach to this whole area. Improvements need to be made, but the Committee should not lose sight of the fact that at the end of the day we are talking to a large extent here about making marketing more relevant, so personally I can sleep at night.

Jed Mole: Alex made a very good point in drawing on the difference between data that is oriented to marketing and other data. If special conditions are created, there is no reason why that data should not be used to tackle that problem. There are two points. One is what data is being used. Then, if we need to tackle major health, financial, social or law and order matters, special conditions need to be created. Deal with it within the realms of the problem you are trying to solve.

- Q14 **Fiona Bruce:** A number of different products can be used. You mentioned baby monitors. There are voice-controlled TVs, devices and toy dolls that we understand can stream very personal video and audio information to companies even outside the EU, where regulation may not be as strong. How can we ensure, for example in a household with children, that data on members of that family is collected appropriately?



HOUSES OF PARLIAMENT

Dr Reuben Binns: You raise a very good point about what are called internet of things devices, such as baby monitors, dolls and TVs. These all used to be devices that we would run locally, so they would be broadcast within the household and no further. Nowadays, these things are connected to the internet, and many of them are very insecure.

When you buy a device, it comes with a default password and you can set the device up without ever changing that password. Many people do so, because it is designed in a way that does not force the user to change the password. That means that right now you can go on to the internet and there are various services that allow you to search lots of unsecured webcams. I can log on to the internet and see webcams all over the world that people have forgotten to secure. There are services that scour the internet to find these open webcams. Some of them are baby monitors; some of them are there for security purposes. There is a bad incentive for companies that make internet-of-things devices not to secure them properly. That is a big concern.

As I mentioned before, websites and smartphone apps often do not write all the code included in them, but include code from third parties with whom they want to allow the sharing of data. The same model is being pushed out to internet-of-things devices. For instance, many smart TVs now contain code from third-party advertisers that is running inside the TV and sending information to them. Similarly, there will be a computer in a smart car, based on Android or another operating system, that allows this third-party code to run inside the car. The same model that we have had for online services, websites and apps is now being pushed out to the internet of things. It is very insecure, and it scary because it reveals a lot of sensitive information.

Fiona Bruce: You are saying that we cannot ensure this.

Dr Reuben Binns: We first need to ensure that products are made in a way that is secure by design.

Fiona Bruce: At the moment, that is not always the case.

Dr Reuben Binns: Exactly, yes.

Professor Victoria Nash: We have just completed a research project looking at how children interact digitally with companies, other than the big tech companies. As part of that, we have looked at their use of things like connected toys. One of our recommendations for policy purposes was that, in addition to the minimum electrical safety standards that we already have for toys, we might in future, as part of the regulation on security of the IoT, have minimum data security standards.

It is worth adding that we recognise that there is a significant problem at the moment. We do not have much resource within, say, consumer protection processes to regularly monitor and check for insecure products. It is notable that Which? in the UK and the Norwegian and German consumer councils have been some of the only organisations to



HOUSES OF PARLIAMENT

speak out and identify significant insecurities in products that are focused on families. My plea, quite frankly, would be for more funding for organisations to ensure the safety of these devices, particularly those focused on children and families.

Q15 Fiona Bruce: You have answered my next question, which was whether there are any special safeguards or procedures in place to protect the rights of younger or vulnerable people, for whom the collection of this type of data might not be in their best interests.

Professor Victoria Nash: You are asking this question at an interesting moment, because we have had the ICO consultation on the age-appropriate design code, which you are probably better able to talk about. We are waiting to see what comes out of that. That may well generate specific protections for minors. in line with Baroness Kidron's recommendations.

Some of the most problematic devices are those targeted at multiple members of a household, including home assistants such as Siri, Amazon Echo and Amazon Dot. We would need to build in safeguards to enable them to recognise, for example, when it is a parent speaking or recording content and when it is a child. I feel that we are quite a long way off that.

Given that you are the Human Rights Committee, I want to flag up one particular concern I have. In putting safeguards in place to protect children and children's privacy, which is what the ICO code intends to do, I really hope that we will not introduce such a stringent code that these companies decide it is not worth them offering their services to under 18s so that children lose rights to participation, expression, information and so on. I would like us to move towards minimum standards that are not too ambitious, certainly not so ambitious that it is not worth a company's while to invest in children's markets.

Fiona Bruce: It is a difficult line, in a sense. How do they get consent for that?

Professor Victoria Nash: You had that debate previously. Consent is an increasingly broken model, and we need much more ethical principles and concepts of best interest.

Jed Mole: If it gives you any reassurance, at Acxiom we have not seen that data made available, at least not mainstream. We have not encountered that. We know it may be possible, but it should be some reassurance that we do not encounter it.

Q16 Joanna Cherry: I have some questions specifically for Acxiom, but first I want to ask a slightly philosophical question.

Jed, you said earlier that we choose to live digitally, but do we really have a free choice? I took evidence this morning in another committee on the EU settled status scheme. That has to be applied for online. Increasingly, all sorts of things have to be done online that could be done



HOUSES OF PARLIAMENT

before on paper or manually. We have all had examples of having to help elderly parents navigate the online world.

Do we really choose to live digitally? Surely, if we are moving away from the broken model of consent, we need to go back to first principles and ask, "Are people really choosing to live digitally? Is there choice here?" I wonder what people think about that.

Dr Reuben Binns: I completely agree with the point of the question, which is that it is no longer a choice. If you want to live in modern society, to interact with other people without being face to face and to conduct commerce, you have to do it online.

Given that that is the case, there is a second question: whether you have a choice between different services, some of which offer you privacy and others that do not. In our research, for example, we looked at applications that would allow you to read a PDF document on your phone. Basically, all the ones we could find sent data to third-party companies. Some of them did so more than others, but all of them did it.

It is the same for all kinds of apps that you might use just to do an ordinary thing like reading a PDF on your phone. Even if you choose to operate your life online, which, as you say, is not really a choice, there is no choice between different services that offer you more or less privacy in a lot of cases.

Madhumita Murgia: It is true. Big companies like Google are now looking at how they can help get people online who have been left out. I went along to their digital garage thing, which is basically a bus that they park up. They had one in Westminster where people could drop in. Often it is older women who have not been in the workforce for a while and might want to come in. I thought of my mum, who would have no idea where to start because this entire process has moved online and she feels completely excluded from it, although she is a teacher and has skills. Technology companies are now thinking, "How do we include people again in this world we have created?", because essentially everyone has to be on there to conduct business and get an education or a job.

Joanna Cherry: Professor, what do you think?

Professor Victoria Nash: How long do you have? It is worth noting that I spend most of my working life speaking about the incredible benefits which the digital world provides. I know we are not focusing on that today. You are quite right: the opportunity cost of not being online is now pretty significant. It is even greater for those in younger generations.

There are two aspects I want to remind you of. One is that we will not get to the point where there is 100% penetration of the internet. There will always be those who choose not to use it, and particularly for things like government services it is vital that there is always another route.



HOUSES OF PARLIAMENT

I do not think you could or should be forced to use the internet. But you are right: for practical purposes, most of us in our daily lives have to be online, because that is where our friends are, where the news is, where the jobs are and where our shopping is. There is no strategy here that simply says, "You will best protect your privacy by not going online", and you are right to shut down that avenue of inquiry.

Jed Mole: I coined the term earlier, and speaking personally we need to do our best to respect the people who do not want to operate online. Sometimes it is difficult, given the nature of businesses, but it is not just about those who want to live online. If people want to opt out, we should do everything we can to make it simple and easy.

The reality is that people find digitally enabled services so convenient that it is hard to resist. By contrast to the app mentioned before, I often travel on the east coast. If the train was late by 30 or 60 minutes, under the delay repay charter I used to have to physically attach the ticket, write in and all those things. Now I open the app, say which train it was, how many minutes it was late, and guess what? It has asked for access to my camera. I take a picture of the ticket, and maybe five days later that money is in my bank account. The digital world can offer fantastic utility and a great, frictionless experience. But we need to respect people who do not want to live that way and to guard against malpractice.

Joanna Cherry: Is it not all the more necessary to look carefully at the rights-based aspects of our use of digital media when it is so hard to resist and it is so prevalent? Does that not make it all the more necessary for us to do what we are doing here today, which is to look at the rights aspects? As others on the panel have pointed out very well, if I may say so, there is not all that much choice once you are on. You can pretty much take it or leave it.

Jed Mole: As Reuben mentioned earlier, taking the app example you are often given a range of things you can say yes or no to. If I am using that LNER app and I get a great family offer, I am pretty relaxed about that, but if it starts making inferences about my financial well-being, my health or anything like that, that is completely inappropriate. We need to segment these different uses of data.

Joanna Cherry: Before I come on to the specific questions for Acxiom, I wanted to ask about something that you said, Madhumita, regarding age discrimination and adverts being placed and targeted only at a certain age group, 25 to 40. If you put an advert in a newspaper—one does not really do that any longer—which did that, it would be picked up, and people like us and the Equality and Human Rights Commission would want to know about it. Who is policing this, policing being a broad term? How did this breach of discrimination law come to light?

Madhumita Murgia: It came to light through investigative journalism, so there was no policing. There was no law enforcement agency looking at it. There were no regulations that they were subject to.



HOUSES OF PARLIAMENT

Joanna Cherry: To take the example of the Sex Discrimination Act, in theory all the hard work of people like our Chair and others over the last 40 or 50 years could be circumvented by targeted advertising online, and we would not know about it unless an investigative journalist identified it. It is pretty shocking.

Madhumita Murgia: Yes. On gender discrimination, gender is one of the most collected data variables. It is collected by everybody. Even if they do not literally get your gender—we can explain more about this—they can infer gender through all the things that we do online as women that men would not. It is one of the easiest things to do.

I read an interesting study by a Harvard academic who said that if you know just three data points about a person—postcode, gender and age—in a database that, as you mentioned earlier, is anonymised, so their name is not attached to it, just a series of numbers, you can with almost 90% probability identify them in a dataset of a million people. If you think about it, how many people of your gender and your age will live in your postcode? It is probably just you. Anonymisation is a myth, and I would be interested to hear what companies have to say about how they keep this data anonymous.

In addition to the question of whether we are consenting to be on the internet, the other question is whether we are consenting to give all our information to companies with which we are not transacting. As we have discussed, it is all right to be shown better marketing, but that is only with the company that you are looking at, are transacting with or have agreed to do business with. Acxiom and many others are not consumer-facing companies, so I would be interested to know on what basis we as users give our data away to companies that we are not getting a service from directly.

Jed Mole: The first thing is a legal basis.

Alex Hazell: Sorry, could I come back to your point? You have hit the nail on the head. This is one of the problems with consent. If someone has consented for their data to be used for marketing purposes and it is then used in a discriminatory way, that consent is probably still sound, although admittedly there might be breaches of other discrimination law.

The better ground for providing more protection against that is an alternate ground available under the data protection rules known as legitimate interests. Basically, that means that you give someone notice—"You permit us to do this"—and you detail what "this" is, which will be marketing and giving some information about that, unless they opt out. It is a form of permission. It does not have to be an active opt-in or affirmative action, but the notice is there. It is available for someone to read. If they do not like it, they can opt out.

The check and balance with legitimate interest that does not exist with the consent ground is that the user of that data then needs to justify its



HOUSES OF PARLIAMENT

use and ensure that its use is not outweighed by any adverse effects on the individual. Back to your discrimination point, if the data is collected under this alternate permission-based ground called legitimate interests, and then discrimination occurs in the way you described so eloquently, the ground is invalidated. You have an extra check and balance over and above any other anti-discrimination law.

Joanna Cherry: How is anyone going to find out that that has happened? That is the crucial thing.

Professor Victoria Nash: That was going to be my question. As academics, this is one of the things we find very frustrating and would love to solve. There are certain things it is impossible to study and research online, and personalisation is one of them. Without seeing the adverts that each and every one of us in the UK receives, it is impossible for me to look for trends, such as patterns of discrimination in the adverts that are displayed, price steering or price discrimination. That is just the way it works.

It is a concern for me, and I would appreciate it if you would comment on this. I imagine responsible, law-abiding companies such as Acxiom are very careful to avoid overt discrimination in the use of your products, but I would be interested to know what checks and balances you put in place to ensure that proxy characteristics do not give rise to discrimination accidentally.

I imagine there is a large array of habits that, for example, women of my generation or my age might use but men of my age might not. I would be interested to know what protections you put in place to ensure, for example, that adverts are not served on the basis of characteristics that are not to do with my gender but which accidentally identify me as a woman.

Jed Mole: I am going to ask Alex to comment a little more on that, because there are checks and balances that we put in place. In leading to that and in talking about being able to identify individuals, the report I mentioned was in the *Harvard Business Review* rather than the UK. A typical postcode has 60 addresses, so in my postcode if someone knew my approximate age and gender it would still be very difficult for them to identify me among all the people who live in 60 dwellings.

Chair: Do they have to have the same birthday?

Jed Mole: I thought the example was age rather than date of birth.

Madhumita Murgia: It was date of birth.

Jed Mole: That narrows it down.

Chair: They would know who you were out of 60.

Jed Mole: Probably, yes.



HOUSES OF PARLIAMENT

Joanna Cherry: I do not understand what Acxiom does. I know you explained earlier that data is actively volunteered to you through competitions—and, I presume, surveys—as opposed to the ad tech model. Can you tell us a bit more about your business model, what service you offer and how you make your money?

Jed Mole: Yes, sure. Acxiom will turn 50 in September, so we have been in business for 50 years. We are headquartered in central Arkansas in the United States. In the simplest terms, there are two halves of the business. The larger part we typically call marketing services, or have for most of that time. We work with a major brand, perhaps a high street brand. They value our expertise in looking across all the various technologies, hardware and software, that are available, to enable them to bring their own data and other data together so that they can understand their customers and prospects.

As you would imagine, they look into the technology that we bring together, interrogate that dataset and say, “We have a new car”—or a new product line—“to launch. These people fit our target profile”. The product is aimed at women, men, people of a certain life stage or whatever it is. They look to fit our profile. It is basically a digital way of doing what people have done from an advertising point of view. As an example, people who sell luxury goods often advertise in business-class lounges in airports. It is the same principle, but it is done at scale using data.

Joanna Cherry: Does the client get actual access to the datasets? Can they go in and look around them?

Jed Mole: Yes. High street retailers, for example, have their own data that they will bring in. Let us say they have a million customers. That is their first-party data, which they have collected on a legal basis, so they are entitled under the law to look at their data to understand their customers. They may begin with the fact that John or Mary Smith bought this pair of shoes on this date for this price, but they may want to expand that relationship with the customer because they do not understand what life stage that person is at or what their hobbies or interests are. A sporting goods retailer, for example, would be interested to know whether someone comes from a family that does lots of sporting activities, as opposed to a family where there is no indication of that.

Joanna Cherry: How do you help them to find that out? What do you offer that helps them to find that out?

Jed Mole: The services side of the business offers the infrastructure and the knowledge to make that happen. On the data side of the business, we have collected publicly available data, data through partners and, in the past, our own data direct, to create marketing data products, and we work with the company to see if we can enhance that data. Do we have John or Mary Smith at the same address? Do we have any information that would help them better understand that customer at that address?



HOUSES OF PARLIAMENT

Joanna Cherry: To take the earlier example, how would you keep that data anonymised so that people are not readily identifiable in the way Madhumita described?

Jed Mole: There are two levels to that. In some use cases, you do not need to keep it anonymised; you need to keep it safe and secure. You need to ensure that it cannot be lost or misused, but if brand X on the high street has a customer who it has legal consent to market to, it does not need to anonymise that in order, for example, to send them direct mail or an email. They may already have that email address.

It is a different use of anonymisation. When someone operating on the internet has not logged into a website and we do not know the person, we try to identify not by the individual but by a group of people, and then do a job that is probably less targeted but is still better than a random job: "This advert is probably more relevant to you than a random ad".

Q17 **Joanna Cherry:** How do you ensure compliance with not keeping data that is excessive, incorrect or misrepresentative? Presumably that is Alex's department.

Alex Hazell: To take a step back, under the new data protection rules there is the concept of privacy by design and default, a new obligation that in layman's terms means that you cannot think of privacy at the end of the product life cycle. You have to build it in at the beginning of the product life cycle and consider it at all stages in the product build.

There is also a new obligation of accountability, which basically means that even if you do nothing wrong, in that there has been no security breach or missed processing, you still need to be able to demonstrate a safe pair of hands. You have an obligation, if asked, to present a suite of data protection policies to the regulator and to be able to demonstrate to the regulator that you adhere to them and they are properly followed within the organisation.

Within Acxiom, we built on our suite of data protection policies that existed in the old world of the Data Protection Act 1998, which was replaced by the new data protection rules last May. We built on that and added to those policies a new set of policies dealing basically with the accountability principle, making sure for example that there was a policy on the threshold in order to carry out a formal data protection impact assessment on a new product, service or change.

To answer your specific question, we ensure that we obtain data in a lawful way by going into the data ecosystem. Literally, we have a team that checks. We do not just rely on reps and warranties in contracts; we actually have a data ethics team that looks at the privacy notices and permission mechanisms used at data sources to make sure that they follow our rules so that all parts of the chain are complied with. That means that we obtain the data in a way that complies with our rules.



HOUSES OF PARLIAMENT

In terms of ensuring the data is not excessive, we have very strict product build rules to ensure that any data that we do not need for the product we either delete or do not obtain in the first place. We are trying to create the optimal product for our advertiser client, so it is in the interest of the business to put as much effort as we can towards ensuring that there is an optimal amount of data in the product. That is carried out by a relatively complex build cycle every three months of our data products in order to ensure that all the suppressions, all the opt-outs and any deceased and bereavement markers can be applied, and that any data that is no longer under licence falls out of the products built from scratch. That is how we ensure that data is not excessive.

In terms of accuracy, Jed mentioned earlier that we are building a picture of propensities and what people tend to like. It is not marketed as, and never will be, 100% accurate. It is a set of propensities that works at scale, but it is not going to be absolutely perfect. Again, we have very detailed build rules to ensure the optimum possible amount of accuracy in the context of the marketing use case at scale. I think that answers your question.

Q18 Joanna Cherry: How do you protect against cyberattacks or hacking?

Jed Mole: We have been in this business for 50 years. Without trying to tempt people who like to hack businesses, we treat privacy and security as incredibly important. To give one example, when new people join the business, they have to take privacy and security training. We all have to pass that on a regular basis, usually annually or more frequently.

Not just Acxiom but almost every business now has consumer data, so this is the responsibility of all businesses. All I can say is that we treat it as incredibly important. We have physical security. We have biometric security. Whatever security we can possibly deploy, we do. We are not doing it once; we are doing it every day and regularly testing ourselves to try to stay at the forefront.

Basically, in the data-driven marketing industry, losing data is the fastest way not to have a business. We know that, we respect that, and we have done that for 50 years. We are doing all we can to be as safe as we can be.

Chair: Thank you very much. That brings our evidence session with you to an end. It has been eye-opening for us, so thank you very much indeed. No doubt our clerks will continue to be in touch with you as we go through the rest of this. Thank you very much indeed.