



Joint Committee on Human Rights

Oral evidence: [The right to privacy \(Article 8\) and the digital revolution](#), HC 1810

Wednesday 19 June 2019

Written evidence from witness:

- [Information Commissioner's Office](#)

3.05 pm

[Watch the meeting](#)

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

Questions 1–8

Witnesses

I: Steve Wood, Deputy Commissioner (Policy), Information Commissioner's Office; Dr Orla Lynskey, Associate Professor of Law, Department of Law, London School of Economics; Natasha Lomas, Editor, TechCrunch; Antony Walker, Deputy Chief Executive Officer, techUK.

Examination of Witnesses

Steve Wood, Dr Orla Lynskey, Natasha Lomas and Antony Walker.

Q1 **Chair:** Welcome to this session of the Joint Committee on Human Rights. As our name suggests, we are a Joint Committee; we are half House of Commons and half House of Lords, and we are concerned about human rights. We are embarking on the question of human rights and the digital revolution, so this is the first session, and we are very grateful for your help. We are very grateful for you coming to us here today to help us set the scene.

We have Steve Wood from the Information Commissioner's Office, which is the regulator. We have Natasha Lomas; thank you very much for coming all the way from Barcelona—you are a specialist technology journalist, which will be very helpful. We have Orla Lynskey from the LSE; you are legal expert on this. We have Antony Walker from techUK, the trade association. Thank you very much, all of you, for joining us.

Perhaps I can start by asking the counterintuitive question. There is a



generalised awareness of the challenges to human rights, issues of privacy and many others, to do with the digital revolution. We tend to skip over how the digital age supports and enhances human rights. First, what is the positive side, in human rights terms, of the digital revolution? How are human rights supported by the advent of the digital age? If they are not, just say they are not, but what is the plus side?

Steve Wood: I am very pleased to be here speaking to you on this topic today. I will give you two examples from our regulatory sphere. The first is the right under data protection law to have your data deleted and how that interacts online with information. The ability of individuals online to delete their information is important, because it enables them to have control. We have the so-called right to be forgotten or right to erasure under data protection law. When data is returned from search engine results and other information that people find online, human rights need to interact in this space; I am thinking back particularly to previous times when you had an ability to forget things. When people went for a job interview, there might have been information that was known about them in the past—perhaps they committed a minor crime that was reported in the local newspaper—and it was forgotten.

Chair: In a way, that is necessary only because of potential human rights problems. Stepping further back, where does the digital revolution support human rights? I am thinking about freedom of expression and being able to do things free from discrimination—not how you are mitigating the challenges to human rights but how human rights are supported by being in the digital age.

Steve Wood: Sorry. I understand your point. My other example of the digital age and interaction with human rights relates to digital identity. I considered talking about freedom of expression but perhaps wanted to give a different example to show how human rights interact in this area.

In this day and age, particularly in an international context when people can be displaced and move across borders, it is very important that people can be identified and have a digital identity in order to enable them to claim benefits or to help or interact with them. Digital technology and even biometric technology, with data gathered online, can enable people to assert their identity. The International Committee of the Red Cross and other agencies can help people to assert their human rights in that context. By interacting online, in an age where people might have found it difficult to establish an identity, they can use these technologies to establish a digital identity.

Natasha Lomas: Thanks to the Committee for inviting me. It is an important topic and I am very pleased that you are taking it on.

To the question, an example is end-to-end encrypted messaging apps, which can help especially people living under repressive regimes to



communicate freely, organise and so on, without interference from the state in that process. That is a gain.

There is still a flip-side, which we saw recently with the protests in Hong Kong when the police forced an administrator of a Telegram channel on the Telegram messaging app to unlock the app so that they could take all the contacts and the messages. Those were protected when they were encrypted, with the centralisation of all the data, but even though encryption is great when it works and it creates all these freedoms and can support human rights, there is still the risk with the centralisation of data that that protection can fall away, and then you have the opposite side where human rights are at risk again.

There is a similar dual effect with social media. It can be great for freedom of expression—it was linked to the Arab spring, supporting democratic sentiment and so on—but since then we have seen repressive states move into the digital space and put a lot of resources and effort into targeting people who are not following the regime. There is a risk of an infrastructure that can be amazing for freedom of speech becoming a control infrastructure if other resources are directed into it.

There are always these two sides. That is important to bear in mind: the freedoms that come from technology are a double-edged sword. There is always an associated risk as well.

Chair: When people are trying to exercise their freedom to organise, freedom of association, freedom of speech, there is always the danger that the state might want to inhibit that freedom, but there is that way of using it first off.

Natasha Lomas: Yes, especially if the data is captured.

Chair: You can make yourself vulnerable as well as empower yourself.

Natasha Lomas: It is evidence, yes.

Dr Orla Lynskey: I concur with Natasha on that point. My research in this area is non-empirical and I tend to look at the challenges of regulating personal data processing rather than the benefits, but it is possible to think of ways in which personal data are processed in order to facilitate transparency and accountability.

You could think here of things like police wearing bodycams to ensure that their actions are appropriate and can later be scrutinised. There is a growing movement in digital evidence gathering in conflict zones, for instance, using hand-held mobile devices and others, with queries about the admissibility of that type of evidence in court proceedings, and follow-on litigation. That is a big potential benefit of these forms of digital technology, if I can be so general.



On a day-to-day basis, the huge facilitating dimension of this comes from the connectivity brought about by digital platforms. Anybody who has ever been frustrated or disillusioned with the way in which their personal data are being processed and has stepped back from a big platform like Facebook or WhatsApp would realise immediately that they lose a lot of connectivity, they lose the ability to chat to family and friends. You can immediately see huge benefits in freedom of expression and facilitating freedom of association coming from digital platforms.

Chair: Your point is very well made that if information can be collected cheaply and digitally, there is less excuse for the state to refuse to share it with the public. A whole load of information that would otherwise have been behind closed doors, in the control of government and not scrutinised is now out there. We have freedom of association. We now have the right to family life. We have freedom of expression. Digital is doing quite well, so far. I know it will take a plunge when we discuss the problems.

Antony Walker: That is a very good place to start the conversation. If you talk to any human rights organisation you will discover that they are very adept in using technology and absolutely depend on it to capture evidence, capture testimony, compile and share evidence, analyse evidence. Human rights organisations tend to be very good at doing all those things.

They also have to be very adept at keeping that information secure, because there will be people who try to access and disrupt it. Many tools have been developed to help organisations collect information securely, share it and so on. Any human rights organisation would say that technology is fundamental to its ability to do its job. In Syria, for example, through the conflict there, an enormous amount of video testimony has been captured that has told the story of the awful human rights abuses that have happened there.

As a tool, it is really important, but the other speakers are right: technology can always be double-edged. Therefore, we have to be very mindful of the way in which repressive regimes in particular or other organisations can misuse the technology to try to infiltrate groups and so on.

Chair: The battle lines are rather drawn up there—a plus side and a negative side. Thank you very much indeed.

Q2 **Ms Karen Buck:** Can I ask you to help us explore some issues about consent, and what you think people understand about consent and where the balance lies?

First, there are some uses of digital technology where consent is required and others where it is not. I wonder if you could help us understand where you think that balance lies.



Antony Walker: There are six legal bases on which organisations can collect and analyse data, and consent is one of those. Clearly it is a very important one, and perhaps the most well understood by the user and the general public, but it is only one legal basis that is used.

It has its limitations. The principal limitation, which I am sure the Committee will want to talk about further, is the user's ability to give meaningful consent, because consent has to be real and has to be for a specific purpose. The challenge is the extent to which users or consumers are asked to give consent for processing and the effect that has on their ability to understand the purpose they are being asked to comply with.

Ms Karen Buck: We will dig down into those issues in a minute, but just pursue that, do most users understand that consent is one of six different legal bases, or do most people think it is the exclusive or dominant issue?

Antony Walker: There is more understanding since GDPR came into effect that there are these other legal bases, but many people will assume that consent is the only form of legal basis, which it is not. There is definitely a gap in public understanding.

Ms Karen Buck: Would anybody else like to answer? You do not have to cover all the same ground, but perhaps there is a different point to make.

Dr Orla Lynskey: To be valid from a legal perspective, consent has to be freely given, specific and informed, so you can already imagine how difficult it is to fulfil those conditions when you think of the way in which you are asked to provide consent in the digital environment. If you are consenting to something on your mobile phone, for instance, that information might be disaggregated across six or seven documents that you have to click through a number of times to get a complete picture of the way in which your personal information is being used. That makes it very difficult to have informed consent.

There is a widespread commercial practice of bundling consent—having very vaguely stated purposes for the use of your personal information, which militates against this idea that you should be consenting to something specific.

Those are just a few of the ways in which consent as a mechanism is put under severe pressure once you try to translate it to the digital environment, which is why it is useful that it is only one of six.

Ms Karen Buck: You are talking about what we would understand as combining data.

Dr Orla Lynskey: Yes, exactly. If you are asked to provide consent to a service, for instance, they might say, "We will provide your data to third parties", so beyond use for their own purposes, but it is often difficult to gauge who those third parties are, what uses they will put the data to—where this data will end up, basically. You can click through further to get



more and more information, but it is very difficult for an individual to get the complete picture when actually giving the consent.

Baroness Hamwee: This question is especially directed at Antony. Is the industry doing anything to make this easier for the consumer or consenter? Sorry, this may not be the right point at which to ask this.

Antony Walker: One of the keys things is making sure that you ask for consent at the relevant moment to enable that informed decision to be taken. It is an important reason why terms and conditions, for example, are not a good means of giving consent, because they are in a very long, drawn-out legal document that will be very complicated. There are definitely ways of doing this right, and the ICO provides very good guidance to companies on exactly that process.

Baroness Hamwee: I was really interested in whether the industry as a whole, the people who make up the industry, are working together. I assume it would be through you. That may not be happening; people may be ploughing their own furrows.

Antony Walker: Following the guidance of the regulator is the best approach.

Steve Wood: It is really important that consent is effective when it is used. Our message as the regulator has always been that if you use consent as your legal basis, you have to meet the tests that Orla set out. However, matching the right context to the right situation, and understanding which legal basis you use, is very important. Generally, there is an overall rule: the more unexpected something becomes, or the more likely it would surprise someone, the more important it is for the legal basis that you seek their consent for it.

It is very challenging online, because an average person might have over 100 data relationships with organisations. That means they may click on a lot of consents at different points of their journey online. If the company wants to use consent, it is really important that the notion is built into what we call user experience and user design. To Antony's point, we know there is a challenge with reading these very long terms and conditions online. Research has said that they are often longer than *Hamlet*.

Therefore, we are urging companies to build the consent process into the user experience, to use the skills and knowledge of these companies. They are trying to design their services to be as attractive and interesting as possible, so we are saying, "You should innovate on privacy and how you do consent in the same way". We are producing guidance on that. We also have a grants programme at the ICO, whereby we provide grants for organisations that can come up with solutions to these difficult problems.

Ms Karen Buck: In practice, it feels recently, post GDPR, that you are



being asked to give your consent in quite up-front and eye-catching ways, and it creates the illusion that you understand what that process is, particularly with things like combining data. In a way, what has now happened is almost the worst outcome. It gives a sense to people that they are being asked to consent, without providing them with any more meaningful sense of what their data is going to be used for.

Steve Wood: We are not complacent about that concern. We know it exists. We are doing significant pieces of work across a number of different sectors and issues. We are doing a comprehensive piece of work looking at behavioural advertising online, those adverts you see alongside lots of different websites that you view, how they use personal data and how you are asked to consent to what is called a cookie, which is the small file that drops on to your computer, as you are often asked to do.

We are looking across that and asking, "What effective information do people need to have to understand that?" We did a piece of research ourselves recently, and we think there is evidence that the public do not understand that interaction. Therefore, as a regulator, we want to work within the law we have, which is the GDPR, and make sure that we make it work more effectively.

It will require us to work with bodies like Antony's more closely in order to drive the industry standards to get things right. You are highlighting an issue on which we have to do more to get it right, because there is that risk of illusionary consent. We want people to be properly informed and for it to be used at the right time and in the right way.

Antony Walker: This is where we are today, with the kind of services we all use on a daily basis. As we go forward, we will only use more and more digital services, so to put all the onus for data protection on the user to give their consent will clearly not be appropriate as we go forward. That is why the other legal bases are so important in GDPR.

Thinking about these issues, privacy does not begin or end with consent. There is a whole body of law here, a whole framework—the GDPR and the Data Protection Act—to govern the subsequent uses of that data, and it does not begin and end with the issue of consent.

Ms Karen Buck: We will probably come back to that.

Antony Walker: As we go forward, we have to think about how else we can ensure that the rights of the citizen and the individual are protected.

Ms Karen Buck: Can I ask Natasha, in particular, although others might have a view on this? Somewhat tragically, one thing that might get people thinking hard about consent and privacy, and how real it is, is an illustration of what can happen when one gives consent without fully understanding what it means. Can you help us to understand whether it has ever gone wrong, and in what circumstances it can go wrong for individuals?



Natasha Lomas: You mean where people have had their data processed in ways that they did not understand.

Ms Karen Buck: They possibly did not understand some of the risks involved.

Natasha Lomas: There are all sorts of examples of not understanding risks, because how data is collected is so opaque and the entire technology industry is very complex. The average consumer has no idea, and the nature of a consent can change quite radically. Facebook, for example, used to have a privacy policy that said it would never use cookies to collect information and track users, but once it gained enough market power it completely shifted that and built possibly the most extensive tracking infrastructure in the western world except for Google.

Chair: Can I pause you there, Natasha? Could you explain what a tracking infrastructure is and whether we would like to be tracked? In responding to Karen's question, what downside and practical impact on this person might there be?

Natasha Lomas: There are all sorts of examples if your information leaks. The rise that we have seen in identity theft and financial fraud, for example, can be linked to the capture of so much data. There is so much data out there.

Ms Karen Buck: Is consent a particular part of that?

Natasha Lomas: It is hard to say exactly, but in some instances that would be true. The data gets passed around so much that it is really not possible for a consumer to understand that, even with these consent principles.

Chair: What is the problem with your data being passed around, and what is the problem with being tracked? We can guess what it might be, but you tell us.

Natasha Lomas: Like I say, identity theft is one example. The loss of privacy itself is a harm. You would not want someone to put a camera in your bedroom even if you could not see it. It is always a harm if you lose your privacy, so to be tracked entails losing privacy. That is the fundamental, 101 harm: that all the things you do in your life can be connected together and joined up, and we now do so much online that it is possible to create a fully fleshed-out profile of who you are, what you like, where you go and who you know.

That is then absolute surveillance. Does anyone want to live under a surveillance state? We can see the extreme example of what that means in China, where the Government are using technology to create a control infrastructure for their citizens, and building scores, so if you do not have a good social credit score you will not be able to buy a train ticket today, or associate with this person.



The extreme risks of having your privacy removed are absolute. It is control by states. It is control by commercial entities. It is all these things. You see a little glimpse of it when your bank loses your information and you think, "Oh my God, someone might steal my money". That is a tiny glimpse of what it is to lose your privacy. It is a fundamental human right, so we have to remember that and defend it, because losing it is a harm; it is a harm in all ways.

Chair: You mentioned freely given consent. If by not clicking the consent you cannot get to the service, or you cannot buy whatever it is you want, is that consent freely given? Is a supplier entitled to make consent a term and condition, which then forces you to consent? Why is your consent freely given in that circumstance?

Dr Orla Lynskey: There is quite a lively debate about that at the moment, and Steve may have something to add on this. The GDPR says that when taking into account whether consent is freely given you need to consider whether, in order to gain access to a particular service, you are being asked to consent to unnecessary data processing. A lot will hinge over the next few years on how much data we consider necessary to provide in this exchange of data when, for instance, I seek to gain access to a service.

The rules do not flat out prohibit preventing access to a service if you refuse to consent. However, it has that condition. To give a practical example of this, the consumer organisation Which? conducted a huge study last year of residents in the UK on their attitudes towards personal data processing. One of its big conclusions was that when individuals access a service online, say a newspaper, and make no monetary payment, they recognise that there is a quid pro quo that involves the newspaper using a certain amount of personal data in order to offer advertising.

There seems to be acceptance of that link, but the question is how much data it is legitimate to extract in order to give access to the free service. At the moment, in practice you see vastly excessive data extraction in relation to the service offered for free. Last week, for instance, I tried to download a supermarket shopping app so that I could order a delivery online, and it wanted access to my photos and all my contacts. In that sense, that type of data extraction could bear no relation to the provision of the contract, but I was being asked to consent to it.

Chair: Which supermarket was it?

Dr Orla Lynskey: The app was Ocado.

Chair: If you did not do that, you would not be able to get your delivery.

Dr Orla Lynskey: Yes.

Chair: I suspect that, for a lot of people who are ordering on Ocado, that



would be news to them.

Dr Orla Lynskey: I had followed up on that by clicking through for more information, but it is a common feature across applications. I have noticed that when looking for law review articles and trying to download an application to see them, and lots of other things. I would not single out Ocado in that way. The issue is systemic.

Chair: They were asking to be able to use photos.

Dr Orla Lynskey: I am not sure for what purposes they would need access to the camera.

Chair: Which photos?

Dr Orla Lynskey: All the photos on my phone. That was my understanding of it; I would need to double check.

Chair: I am sorry, Orla. If that is your understanding of it, it is good enough for us. That was a shock.

Q3 Joanna Cherry: I want to explore a bit more the idea of informed consent and whether meaningful consumer choice is really an option. Before I do that, I notice that in its written evidence to this inquiry the Law Society of Scotland argued that some privacy policies, which explain how the data will be used, are so long and complicated that they are in breach of the law, in so far as the law requires privacy policies to be concise, transparent, intelligible and easily understandable. Some of these policies clearly are not.

Would any of you like to comment on whether Law Society of Scotland has gone too far there, or whether it is a fair comment?

Antony Walker: I would make a distinction between privacy policies and terms and conditions.

Joanna Cherry: I would entirely agree with that statement for terms and conditions, but this was specifically about privacy policies.

Antony Walker: Absolutely, privacy policies should be clear and understandable. That is what they are there for. The best practice should be that they are relatively short, use plain language and are clearly understandable. Terms and conditions, on the other hand, are essentially a legal contract. Therefore, they are required by law to be long and complex, and they always will be.

It is right that the focus should be on the clarity, readability and accessibility of those privacy statements, to ensure that they are as meaningful as they can be.

Steve Wood: From our perspective, in regulating this area, we are advocating what we call a layered privacy policy. The key information



that the user should know should be at the top layer, and spelled out very clearly and effectively when the user interacts with the service, so they can drill down and find more information below that. That is not happening everywhere. Some improvements have been made since GDPR came into force, but there are examples of unclear wording in the information given to someone when they are consenting.

We called out this vague notion of what are called “third parties”. What does “a third party” mean? We have now taken action in a number of cases recently. We took a case against Bounty; you will be aware of Bounty, the provider of information and baby paraphernalia—nappies, et cetera—when young mothers are in hospital. They can sign up to that either via an online service or on paper.

We concluded an enforcement action against Bounty this year and fined it £400,000, because the information given to people when they were signing up and allegedly consenting in that situation referenced third parties, but that information was actually going to credit reference agencies. We felt that was not a clear and meaningful explanation. Therefore, we were concerned about the risks to an individual who did not realise that their information was going to a third party like that. As a regulator, we are calling out those examples and saying that in that situation the information was not clear and it was not informed consent.

We have a role as the regulator to call out those examples. Equally, we are stressing in our guidance that we expect that clarity very early on in any interaction. We know that people’s attention online is very short; it is a different environment from the analogue world people were dealing with 20 years ago, so how do we make consent work in that space, if it is to be used? I accept Antony’s point that if we use it too much it can become devalued and less effective.

Joanna Cherry: You are talking about a layered approach. Even if there is a layered approach—starting off with ticks and boxes that are easy to understand so that someone can understand what they are really signing up to and what their rights are—surely they need to understand the privacy policy. This is what the Law Society of Scotland said. A lot of these privacy policies are so long and complicated that they are really not concise, transparent, intelligible and easily understandable, so there is a fundamental legal problem there.

I notice that research was done for the BBC last year looking at companies like Amazon, Apple, Facebook, Google, Instagram, LinkedIn, Snapchat, Spotify, Tinder, Twitter, WhatsApp and YouTube. The research said that their privacy policies were written at a university reading level and would be more complicated to read than Charles Dickens’s *A Tale of Two Cities*—I am not sure why that was singled out. Of course, not everybody has that reading level, and even those of us who have been to university might not want to be faced with that in order to understand the privacy policy. Is there a meaningful way around that?



Steve Wood: We have given examples of how companies can do it differently. They can provide online videos with this information. They can provide little snippets of information against the online form when people are signing up. We are expecting them to innovate in the online space to make sure that the information gets to people at the right time.

Equally, if the information is buried or in very legalistic text, that is a problem, because the GDPR, our new law, which came into force last year, makes very clear that it is meant to be in clear, plain, accessible language. Due to the scale of the challenge, as a group of regulators we are tackling this at European level. You talk about all these really large companies. To the issues that Orla was talking about, over the next few years we will have a number of precedent-setting cases. Some of them will come out at a European level, because the general data protection regulation is being implemented across Europe, and there is a European Data Protection Board, which the ICO is part of, to implement it.

A lot of the key companies are based in Ireland; in the UK, for example, we get our services from Facebook Ireland. A lot of these cases will be driven at European level, and we have to start to determine these questions, show where the line needs to be drawn and draw out these practices. There is more to come as we start to tackle these issues.

Dr Orla Lynskey: I concur with what Steve said. In particular, a very big judgment is pending before the European Court of Justice at the moment, in a case called Planet49, on exactly this question of how much data it is appropriate to provide in order to avail of a free service. In that case, it is a lottery that is offered for free or without monetary payment, and in exchange the individual is required to receive advertising from 30 commercial partners.

The hint from the Advocate-General in that case is that that is an appropriate exchange. However, I would query whether that is in line with the principle of data minimisation. It strikes me as quite excessive in exchange for the opportunity to participate in a lottery service. You can see that the question of how much data is appropriate to extract in a given context is a very difficult one to answer. In some respects, there is a value judgment there.

Antony Walker: The reality of all this is that these issues are complex for getting the balance right. It is important to recognise that we now have a legal framework in place, across the whole of the European Union, that provides a basis for precedents to be set about exactly what these things really mean and what the primary legislation means in practice. It is true: there is an expectation that over the next couple of years through case law we will start to see what the correct norms around all these things are, which will help move the market to the right place. The importance of having GDPR there really should not be underestimated.

Chair: Following up on that point, we are all familiar with the



responsibility on the consumer to inform and protect themselves, and with the idea of caveat emptor: buyer beware. It sounds to me, following on from Joanna's questions, that in this situation the consumer, who needs to have university reading level-plus, has to click through loads of things and have Orla's level of expertise in order to get something, and needs to have masses of time, like 26 working days a year, to read privacy policy, is not in a position to defend themselves.

Does it make this a situation where, although it is the consumer's right to privacy, in order to protect that right we need the state, regulation, law, clear rules and enforcement, because we cannot do it ourselves? I am feeling quite relieved about this, because I am not doing any of it to protect myself. Do we not need a big, mighty protection? Is that you, Steve?

Steve Wood: We have been given stronger powers under the GDPR. As Antony said, it is Europe-wide now and these powers are consistent across the EU. We have the power to fine up to 4% of global turnover, which has moved data protection from a lower league type of regulation closer to areas like competition that can really call out the most significant, systemic breaches, which may sometimes involve hundreds of millions of people's data. The regulation is scaling up.

The other concept I wanted to talk about, which has not been mentioned yet, is rebalancing. You are right: we cannot push it on to the consumer to make all these decisions and think that those are the sole safeguards. It is the concept of accountability: to hold accountable the companies that process the data. The other strong provisions in the GDPR are to require these companies to take a risk-based approach. It is for them to assess what the risks are in reusing the data. Would that be expected? What potential risks or harms would that cause?

There is a provision in the law that requires the companies, in certain situations where they detect a risk, to conduct what is called a data protection impact assessment, which places the accountability on the company to do that. We can ask to look at that as a regulator. If we go in to audit one of these companies and look at practices, we can ask, "Have you done a data protection impact assessment? Have you taken account of the risks, issues, concerns and impacts on the consumer in using the data in this particular way?" That accountability, that rebalancing, is very important in driving this forward.

We are saying to organisations, "This is about trust with consumers". There is a bit of a business model issue here: ultimately, people will become more concerned about providing data, and you will not be able to use this data in your business model. If societal and public concern grows, you need to develop their trust as well, and you do that by being more accountable. We are trying to bring that together. That is the other piece of the jigsaw in making this work.



Q4 Lord Woolf: I have been listening to this with great interest. It seems to me, having heard what you have been saying, that it should be based on informed consent. That sounds very well in principle, but it seems to me that it is very difficult in practice for the consumer to know the consequences of doing what apparently is giving consent. I wondered to what extent the regulator is funded to educate.

Steve Wood: That is another really important question. In the advent of the new law coming into force last year, we ran a public campaign, which we called Your Data Matters, not to use jargon about what the law means in legalistic terms but to get people to have a wider awareness about how their data could be used by organisations and some understanding of their rights, and equally to explain the obligations of the organisations in starting to raise people's awareness.

That digital education part is really important, but equally the responsibility needs to be on each company to be open and transparent. We have also provided information about how they can reuse our campaign with their customers.

Lord Woolf: Do you carry out surveys to see how your guidance is being employed by users?

Steve Wood: In terms of the public, we run an Annual Track survey, which tracks the responses of consumers to issues of privacy and data protection, which we can make available to the Committee if that would be of interest. Last year, we saw an increase on the question of trust and confidence. We think that is partly because of the introduction of the new law. It is too early to know whether it is starting to have an impact, and I would not make any claims from the first year, but it is very important to measure and track whether the things we do are having an impact. We are happy to share the data we have with the Committee if you are interested to see it.

Q5 Baroness Hamwee: I should declare that I took part in the passage of the Data Protection Act through the Lords, without, I have to say, entirely understanding what we were talking about, so I really did not give informed consent to what was going through.

Can you talk about whether the law does enough to protect people who may be in a particular difficulty in giving informed consent? I do not just mean people with university-level reading skills. There are specific questions about children and people with learning difficulties. I do not know who would like to start. Maybe, Steve, it is another one for you.

Steve Wood: I was hesitating, to make sure I do not dominate. Those are really important issues. I will discuss children first and turn to other vulnerable groups after that. It was a really important step forward for the GDPR—compared to the data protection law that we had before, the Data Protection Act 1998—that it explicitly referenced the importance of protections for children for the first time. They are referenced in a



number of the articles on consent—Article 8, for example—and in a number of the recitals. It sets out the position that treating children as adults online is a significant issue, and we have to think about the risks that have emerged. The internet was not built with children in mind, so how do we address that? It is a tricky question.

The approach we have taken in the UK is to add an additional provision to the Data Protection Act 2018, which was brought forward by Baroness Kidron. She advocated for this provision, which is for an additional piece of guidance, a statutory code of practice, to be produced by the ICO. That is an age-appropriate design code, which is meant to set out how we design online services with children in mind.

What should we do to take account of services likely to be accessed by children? This is not just a question about consent, because consent is part of the equation, but even if there is consent from, say, a child of 14 or 15, or their parents' consent on their behalf if they are younger, you want to make sure that they are safe throughout their time online. Consent is only part of the process.

In the draft of the code of practice we published for consultation recently, we look at such things as default settings. Should the geolocation, the geographical tracking built in to a lot of online applications, be switched off by default? Therefore, it provides a safe space for children to learn whether they want to switch these things on and explore online. It is a really tricky topic. As a regulator, we have to learn to tackle that. There are some provisions in the law that we think are helping, but it is a significant challenge that we will put a lot of effort into over the next five years. We have some positive indications and positive starters in the new law.

Baroness Hamwee: Does anyone else want to talk about children? Then we will come back to people with learning disabilities, perhaps. Maybe you can tell us when the guidance is likely to become effective.

Steve Wood: We published a draft in April, which has been out for consultation. The consultation has just closed, so the new code of practice will be published in the autumn.

Antony Walker: These are really important provisions both in GDPR and in the Act itself. One of the challenges we have is that there is no watershed moment when a person goes from being a child to an adult, when you think about online services. Take the issue of geolocation data or GPS data. As a parent you may well, for a child's safety, think, "Actually, I quite like my child to be able to get an Uber home from an evening out", for example. That child may be 17 or 16. If that child cannot use location data on their phone, they cannot access that service, so you cannot arrange that transportation home.



These issues need to be thought through. What are the services that we want to make sure our children have access to, for their safety, their education and so on? In the code, we must not end up with some catch-all thing that has unintended consequences as well as safeguards. We are responding to the consultation, and we are very keen to get that right, but it is tricky. There are detailed and specific issues that need to be thought through.

Baroness Hamwee: Orla, do you want to help us with the age of consent? The UK decided to put it at 13, not 16. You will have an international perspective.

Dr Orla Lynskey: The UK was one of, I think, six European countries that opted for the age of 13. Different rationales were put forward by different countries for choosing that particular age. Settling on any age is quite difficult, because you look at things like the capacity and developmental progress of a child, their educational needs and socioeconomic background. My colleague at the LSE, Sonia Livingstone, is doing a project funded by the ICO and has highlighted that all those factors are relevant when considering whether it is appropriate to ask for a child's consent in the digital context.

Even beyond the age of 13, between the ages of 13 and 18, the processing of personal information of minors might be riskier than other forms of processing. That type of thing would need to be taken into account in the impact assessment that Steve had mentioned. In all the non-legal research that has been done in this area, drawing on developmental psychology and other things, the emphasis is on ensuring that children are not restricted in their use of technology or closeted in the way they are allowed to use it.

There is data, again provided by Livingstone and her team, to show that you should moderate the use of technology in an enabling way rather than simply saying, "You cannot access this app and others", because in some ways children need to become streetwise in this context. It is not simply a question of preventing access to these services. It is a question of ensuring and facilitating access, but then having all the backstops in place that Steve has mentioned: strong enforcement in case of blatant violations, data protection impact assessments that can be audited, and all these other things, to support children when they are acting in this environment.

Natasha Lomas: It is important to remember that a lot of children under the age of 13 are online, looking at videos on YouTube, and this is the reality we live in. This is on platforms that perhaps know us better than we know ourselves but that also apparently cannot, or will not, identify an underage user. There is an interesting tension there: they know everything about us for their own ends, but when it might be beneficial to society not to let a six year-old watch a video on YouTube, they do not use that data.



Baroness Hamwee: You were going to come back to people with learning disabilities.

Steve Wood: Yes, I can return to the other group. It is an important question, and we probably would acknowledge that we need to do some more work there. We had feedback recently, in our consultation on age-appropriate design code for children, about groups with learning disabilities. We are taking that away at the moment and thinking about it. We already have a stream of work and a priority area at the ICO on vulnerable groups and how their data is used. It can probably form part of that work.

In a number of circumstances, particularly if you are sharing the data of someone with learning difficulties or a vulnerable person, consent will not be the most appropriate basis, which is why the law provides for other legal bases. Sometimes, for example, it might be in the vital interests of that individual that the data is shared, certainly in a safeguarding type of situation. The law provides for other legal bases, but it is very important that there is the impact assessment and the consideration of how that is going to impact on the individual.

We have also worked with charities in the past. We have worked with the Alzheimer's Society on issues with people's data when they have reached that stage in their life or had a life-changing circumstance where it may be difficult for them to consent, which happens in the analogue world. We are also looking at how those issues can affect data. It is a complex issue, as with children. We need to work with the experts to provide more specific guidance, but we are working on it.

Baroness Hamwee: It strikes me that we are all vulnerable, actually.

Q6 **Lord Woolf:** I wonder if Orla can help me. How does the law work in this area? If the test is consent, who has the onus of sharing consent?

Dr Orla Lynskey: The law places responsibilities on data controllers. They are the entities that determine how and why personal data are processed. Under the GDPR, it is now a legal requirement that they are able to demonstrate that consent has been obtained, and that forms part of this principle of accountability that was introduced by the GDPR. The focus has moved. Although individuals still have that possibility to consent and are given mechanisms to exercise control over their personal data, there has been recognition in the law that that is not sufficient, and in some ways it overburdens the individual. That is through the introduction of these other mechanisms that facilitate auditing and compliance, to ensure there is more transparency around personal data processing, and then stronger fines and things like that.

Lord Woolf: That is a very helpful answer, and I thank you for that, but I am wondering how you know whether they are doing what is required.



Dr Orla Lynskey: That is a very good question. Individuals have certain rights under the framework. For instance, you have a right to access your data. You could put in a request with a data controller to see on what basis they are processing your personal information. You might be able to gain access that way yourself through a bit of investigative work, but the key thing to note there is that it requires the impetus of the individual to actually do that.

One of the key omissions or failings of the GDPR is that data protection impact assessments are visible to regulators but not to the general public. That means external scrutiny of them by NGOs, academics, or others who might be interested in trying to get a grasp on what is happening is difficult.

Q7 **Lord Trimble:** There have been quite a few mentions of the GDPR so far this afternoon. Do the GDPR and the Data Protection Act 2018 provide a good enough legal framework for processing data?

Antony Walker: When we work with global technology companies, there is a view that it is probably the strongest and the deepest data protection framework anywhere in the world. It is world leading. It is seen as the highest bar, and it is the bar that many of the largest companies set their global compliance around. For example, some very large US multinationals have fully adopted GDPR as their own framework for their global operations. It is the best that is out there.

GDPR was always going to struggle a little in keeping up with innovation and changing technology, although it has been written and put together in a way that, I hope, enables it to evolve as services and practices develop. We are only in the early stage of its implementation, and we are yet to see the case law come through that will further refine the law and provide greater clarity to businesses, regulators and citizens. This is the start of a journey, but GDPR is probably seen as the most stringent framework anywhere in the world.

Dr Orla Lynskey: I agree with that. It is impossible now to assess whether it is good enough yet, because we have yet to see how it will be implemented through decision or practice of regulators, or interpreted by courts. The fundamentals are very positive. As I have said, one thing I personally regret is that the legislation does not provide the tools for those who are not regulators, but academics, civil society organisations and others, to get a better grasp on actual data processing practices. There is a shadow data economy that is not necessarily visible to the external eye. In order to hold it to account and see whether it is lawful, you need to have a little more transparency on those practices.

It would be really useful to have something similar to or along the lines of financial or security disclosures—the types of public disclosures that are made by big companies in the US—for data processing practices in the



EU. The GDPR does not really give us that. It puts a huge burden on regulators, in fact.

The other regret I have about the implementation of the GDPR in the UK is that it provides an opportunity for civil society organisations or non-profit organisations to take representative actions on behalf of individuals before supervisory authorities or courts, but in the UK at the moment you have to have the mandate of the individual to do that. The GDPR left open the possibility that member states could allow for this without the mandate of individuals, but that option has not yet been taken up in the UK. That is under review; it will be reviewed again in about 18 months.

Allowing civil society organisations to act on behalf of individuals and take representative cases without their mandate would be a very powerful tool. It would go a long way to removing the burden from individuals for protecting their own rights, and would complement the work of regulators very well.

Lord Trimble: You mentioned that the regulation under this legislation is very stringent. Is it too stringent?

Antony Walker: Some would certainly argue that that is the case. There is a big debate in the US at the moment about how they address those issues, and some are arguing that the US should have a similar framework at a federal level. Many are making the case that GDPR is too stringent. In the run-up to GDPR being implemented, many in business and industry said it was going too far.

It is quite interesting that, once it entered into law, a lot of people became reconciled with it as it is. They feel that it is the right approach and these are fundamental issues. It is fundamental to have an environment where you can operate with the trust of your consumer and so on. Many companies that were probably sceptical have become quite reconciled to it and are trying to work with the letter and the spirit of GDPR. That is my assessment.

Lord Trimble: Are there any additional measures, practical and legal, that we should consider to improve the consent process for all the parties involved?

Steve Wood: I am happy to answer that briefly and perhaps build on one of the answers I gave earlier. Working with industry is very important. As a regulator, the ICO is horizontal, so we cover the public sector, all parts of the private sector and the third sector, developing standards that work in the context of those industries.

If typical companies in those sectors that rely on consent are developing more standard practice, which has been validated and looked at in the round, and indicating that it is a good standard that should be followed, it can be driven by certification mechanisms set out in the GDPR. You can



certify the data protection practice of organisations. We need to do more to drive forward these standards to show what good consent practice looks like. There is more work to be done to get it right in this context so it works for consumers on the ground.

Q8 Chair: In conclusion, we have heard from you that there is a very big job to be done on our behalf, as the consumer, in respect of our human rights to privacy. Research has to be carried out by Orla's colleagues. Court cases have to be taken to challenge people who are overstepping the mark. Industry standards have to be developed. There has to be digital education. Orla talked about the huge burden on regulators.

The digital revolution is driving productivity and profit in the sector. Does the public purse pay for all this, or is there a levy on your profits so that the taxpayers do not have to pay for the protection that they need in order to engage with you and drive your profit? Should you be paying for all this or do we have David and Goliath there? Presumably it is a multibillion pound industry with billions of users. I should imagine that the Information Commissioner's Office is quite a small unit compared to that. Is there a levy on you to pay for this, and if so how much is it and who do you pay it to?

Antony Walker: Steve probably knows better than I do.

The Committee suspended for a Division in the Commons.

Antony Walker: The ICO is funded by a fee that is levied on the data controllers, so, yes, it is paid for by the businesses. It is really important to stress that the digital economy is not just the big data companies; it is the whole economy. In order to protect our rights, it is essential that we look at this from a whole economy perspective and not just a subsector of the economy. Steve will be able to explain a bit more about how the fee is calculated.

Steve Wood: As a regulator, we are funded by a fee, which all data controllers—data organisations that process and hold personal data—have to pay unless they meet an exemption, which is generally there for your smaller businesses, because it is not fair to make your hairdresser pay it. It is proportionate in that context. The fee is tiered, so it focuses on the larger organisations, which pay the high fee of £2,900. There is a fee of £90 and another fee of £45. The organisations are divided, based on their turnover and number of employees, into those three tiers. That makes up our overall budget.

We had very positive discussions with government, during the passage of the Data Protection Bill through Parliament last year and the introduction of the GDPR, which allowed us to substantially increase our budget. We are moving from having 400 staff before the introduction of GDPR to closer to 700, with the ability to go up to probably 800.



We know we have to hire more technologists, people with the background and skills to deal with these issues. We have just hired our first AI fellow from Oxford University to bring more experience into the ICO. That funding is very important to us, because it is our sole funding for our data protection work. We do not have any grant in aid, but we have that level of fee. We can also make the case to go back to Government if we need more money, for example to have the fee increased if we need to have it funded in that way.

There is a wider debate as well in the context of online harms. The online harms White Paper was composed by the Government earlier this year. As for the regulation beyond that, whether there is a need for a technology levy or a levy on the industry has been raised and discussed by other committees, including the DCMS Select Committee, but we have not commented on that in the context of data protection.

It is the principle that the polluter pays, and that is inherent in our system in that the largest companies pay more. It may need to evolve and change over time, depending on how important and complex this digital regulation gets, to make sure that we have the resources to do our job. I would like to report a positive conversation. We are a public sector regulator and we are expanding, which in this day and age is quite rare, so we have been supported by the Government to get the extra funding we need.

Chair: Before we finally conclude, are there any examples of incursion into human rights in relation to digital activity, Natasha, that we should be thinking about that we have not yet touched on?

Natasha Lomas: Inferences can be made from personal data. You give your pieces of data and you think that is all you are giving, but using AI technologies all sorts of inferences can be drawn from this information. New companies might then calculate certain things about you that you do not necessarily know they are doing. Some relatively recent research showed that by using a dataset of selfies from a dating app, people created an AI that could predict more accurately than a human whether somebody was gay or straight, for example. You are putting your photo on a dating app, but AI technology might be being used to figure out your sexuality.

That is a really big issue for privacy as a fundamental right. How can you expect, when you put a selfie online, that somewhere down the line a company might use it to determine your sexuality, which is a very sensitive type of data? It is protected as a special category of data under European law.

All sorts of inferences can be drawn from the information we put out there. There are other examples of research on VR looking at the first-person perspective, eye tracking and, again, determining somebody's sexual orientation, or trying to figure out whether they have mental



illness, are drunk or have taken drugs. You are just using a piece of technology, and it might be making all these calculations about what it thinks you are, which might be wrong. If you do not even know it is happening, how could you address that inaccuracy? They might be telling someone else and sharing this inference that you are a drug taker, and it is not true. There are huge implications based on how powerful these AI machine learning technologies are now, and how they can transform our data into all sorts of inferences.

We do not even see that happening. We do not see the algorithms at work. We do not know what they are doing. We cannot get that data. We have talked a bit about having rights under GDPR to get our data, but the issue is that frequently the companies define personal data very narrowly and in their own interests. Facebook does this; it has a button where you can download your data, but it will just give you the things you have literally uploaded. It will not give you all the inferences that Facebook has made from your data, everything it has learned by watching you continuously. It does not define all the surveillance and intelligence as your personal data. Under GDPR it should, and this will be highly challenged. I hope regulators will come down hard on it, but that is the situation we have now. How can you possibly know what is being done with your information behind the scenes? It is a huge, huge problem.

Chair: Thank you very much, all four of you, for coming and helping us in this first session of our inquiry. I am sure that our very excellent clerk team will be back to you relatively regularly to pick your brains as we go through this very important inquiry. Thank you very much indeed.