HOUSE OF LORDS

Select Committee on Democracy and Digital Technologies

Corrected oral evidence: Democracy and Digital Technologies

Monday 16 March 2020

3.05 pm

Watch the meeting

Members present: Lord Puttnam (The Chair); Lord German; Lord Harris of Haringey; Lord Holmes of Richmond; Baroness Kidron; Lord Lipsey; Lord Lucas; Baroness McGregor-Smith; Baroness Morris of Yardley; Lord Scriven.

Evidence Session No. 23 Heard in Public Questions 289 - 296

Witnesses

I: Elizabeth Denham, Information Commissioner; Steve Wood, Deputy Information Commissioner.

Examination of witnesses

Elizabeth Denham and Steve Wood.

Q289 **The Chair:** Welcome and thank you. Sorry for the slight delay. We overran a little on the previous session. I will read the police caution and then ask you to introduce yourselves. As you know, this session is open to the public. A webcast of the session goes out live and is subsequently accessible via the parliamentary website. A verbatim transcript will be taken of your evidence and put on the parliamentary website. You will have an opportunity to make minor corrections for the purposes of clarification or accuracy. Lord Mitchell is in self-imposed isolation, but he is watching us, and if he has a question, we will get it through and I will repeat it. Would you introduce yourselves for the record and then we will go to the first question?

Elizabeth Denham: Good afternoon. I appreciate the invitation to speak with you this afternoon. I am the Information Commissioner for the United Kingdom.

Steve Wood: I am Deputy Commissioner, responsible for regulatory strategy at the ICO.

The Chair: The first question is from Lord Scriven.

Q290 **Lord Scriven:** Do you feel that you have sufficient powers and resources to protect against data misuse and to conduct data audits of political parties and technology platforms? I am particularly interested in the powers, not just the resources, when you answer that. Do you think that more auditing of the political parties and large tech platforms is desirable? If it is, how would you go about doing it differently or at quantity?

Elizabeth Denham: We are fortunate as a regulator to have had a modernisation of our law in 2018. For 20 years we had the Data Protection Act 1998 and now we have the Data Protection Act 2018, which provided for new powers for the office to make us a fit-for-purpose digital regulator. It was helpful to have the powers of audit, the powers to be able to carry out no-notice inspections and the powers to be able to query algorithmic decision-making. All these powers go a long way to help us in our regulatory job.

When it comes to resources, in 2018 we were also given a new fee regime, which allows us to build the capacity to do the work. A new fee regime, new powers and modernised law are all very helpful tools to take us forward. When it comes to audits of political parties, we have the powers to audit any organisation. The powers of audit are not always a punitive power. Many times, we are invited into an organisation to carry out an audit which it finds helpful in getting data protection right. We have carried out audits of all the main political parties, and the result of them will be published in due course.

To carry out the audits, we needed to talk to the data protection officers for the parties, talk to the party officials, find out exactly what the source is of the data that they collect, and we run the practices by what we think is required to meet the compliance obligations of the UK data protection law. We are really fortunate in that we can audit not just in the regulated period of party activities but 365 days a year and get to the bottom of the data aspects of political campaigning.

Lord Scriven: Are you totally happy as a regulator that you have all the powers and resources necessary to carry out this work, or do you see gaps both in what you do, or gaps in terms of regulation that you would like to see changed which would help you in this process?

Elizabeth Denham: Every regulator can always make a case for additional resources and additional powers, and I would not hesitate to come to government and Parliament if we felt that we needed new powers to be able to carry out our important function in the public interest. My point is that we have had a modernisation of the law which other regulators that are working in this space have not had. The Electoral Commission, for example, needs an update in its powers and resources, and the kind of compliance tools that will drive good compliance.

As this Committee is well aware, we had a maximum £500,000 fine for significant contraventions of the law, and it is now up to four per cent of global turnover. That is a significant power to be able to drive compliance, especially of the large tech companies. I would not hesitate to come back for more resources and more powers, but we were given in 2018 the gift of a range of sanctions and powers to use as a proportionate and rational tool to drive compliance. Sometimes that is a stern letter from the Commissioner, a letter of warning. Sometimes that is a fine. You will have seen some of the fines that we have levied in the last year under the GDPR and Data Protection Act 2018. However, some of the other regulators working in this space have been left behind. All of us need to be brought up to a level playing field to be able to reach across borders, to be able to carry out interjurisdictional investigations, because, as we know, the challenges around democracy and data that we all face are not domestic challenges; they are multijurisdictional. We need that extraterritorial reach. We need the kinds of sanctions that the change in law has given the Information Commissioner. We need a level playing field to really tackle this set of societal issues.

Lord Lipsey: Among the armouries that you have at your disposal, there are statutory codes of practice of course which you can apply. How do those assist you? Are there any other statutory codes you would like added to the statutory codes you have at the moment?

Elizabeth Denham: Under UK law, we have a requirement to compose four different statutory codes. There is the Age Appropriate Design Code, which is the children's code. It is world-leading work. We have filed our code on age-appropriate design with the Secretary of State to be laid before Parliament. We are also tasked with updating the direct marketing

code and producing a data-sharing code. The fourth code that we are working on is a code for data protection and media. For all those statutory codes there is an in-depth consultation period where we talk to stakeholders and take into account their responses, and then it is up to government to table the codes.

I also want to highlight that all those codes land in an area where there are competing rights. If you think about the media code, that is about balancing freedom of expression and the right to personal privacy. If you think about the children's code, that is about protecting our kids online while still allowing businesses to provide their services and freedom of expression in terms of media.

When it comes to political campaigning and data protection, we have drafted guidance to tackle the issues around the ecosystem of players who are collecting data and using data in campaigning. That is not a statutory code, but we think it is a candidate to become a statutory code in the future. We are blessed with having some time to turn that guidance into a candidate for a statutory code. Ultimately, that is up to government and Parliament, but we have done the work. That guidance is of interest to many other jurisdictions which are looking at these very same issues around data and democracy.

Lord Lipsey: The political parties will tell us that they are totally protected by the Data Protection Act — I cannot remember which clause it was. Are you saying that you would welcome an extension that makes it clear they are not quite as free as they think they are?

Elizabeth Denham: The exemption that you are referring to concerns democratic engagement. That provision allows the parties to be able to balance that interest of engaging the public, especially using digital tools, knowing how important that is, and at the same time protecting personal information. The democratic engagement exemption does not exempt the political parties from the other principles of data protection. We are working closely with them, but they are not the only players in the ecosystem, as you know. We are dealing with social media companies, data analytics companies, data brokers, et cetera.

Steve Wood: Given the complexity of the ecosystem, we hope that the guidance will be helpful for political parties because they have a greater array of tools at their disposal than perhaps they had 10 years ago. They have always had the spine. They are entitled to have the electoral register. Essentially, that is a dataset on the entire UK adult population. It is very important that political parties have that because they need to understand who voters are. However, there are some bigger questions about fairness and transparency, about how much data you should build on to that spine from other sources, and how that interacts with other parts of the ecosystem, such as using online platforms to do behavioural advertising online. The guidance provides clear guidance to all the actors in the process. We would see it as a levelling of the playing field. It is helpful, because it means everybody understands the regulator's interpretation of the law. On the concept of "necessary for … democratic

engagement" in Section 8 of the Data Protection Act, it is best that more information is provided around that to help explain what parties can do. We want it to be enabling and not to put barriers in place, but, equally, to talk about where there are risks and where we think the law needs to engage with those risks.

Baroness Kidron: You have gone ahead to a question which I was going to ask later. Let me ask the last little bit of this one, which is: have you had any support for this approach? Where has that support come from?

Elizabeth Denham: Are you referring to the support for that particular guidance?

Baroness Kidron: For that particular code, for the work that you did in 2019 and previously.

Elizabeth Denham: It dates to the 2017-18 investigation we carried out. Many of you around the table will know about our investigation into Cambridge Analytica and Facebook and data brokers on the use of data. The issue was of concern to Parliament, policymakers and citizens. As a response to those concerns, we pulled back the curtain and in our report we really examined the use of data for micro-targeting, for profiling of citizens and voters, and what the implications were.

We had a lot of questions from the political parties, because again, as Steve Wood just said, these are new tools and five or 10 years ago, behavioural advertising was used by commercial players, but not necessarily by political parties and political campaigners. Those methods have morphed into use by political parties. We really wanted to level the playing field and give assurance to political parties and others as to what the law really says.

The support that we have for putting out that guidance has come from jurisdictions around the world which look to the UK as a leader in unpacking some of these issues. You will know that there was a grand committee of parliamentarians from the 11 or 13 jurisdictions that were looking at these issues. We spoke to not just this Parliament but the Canadian Parliament, because it is looking at an inquiry on the very same issues and improving its law and its guidance around this.

We do not have all the answers. Nobody has all the answers, but the jurisdictions around the world — G7, G20 — are looking at data and democracy as very important issues. We have support around the world and from other regulators. I chair the Global Privacy Assembly, which is a group of 130 data protection authorities around the world. The use of data in democratic campaigns is a live issue that has come across our desks at the conference and has been the subject of resolutions.

Q291 **Lord Harris of Haringey:** In the answer to Lord Scriven's question, you pointed out the very substantial increase in your power to fine which is now going through. That relates to the larger actors in all this. However, we have also had it put to us that in terms of bad practice during election

periods, it is often much smaller, niche actors who are targeting voters in a particular way. It is very unclear why, how, what data they are using and so on. There is a danger, is there not, that because you focus on the very big actors, and of course the very big actors are very powerful and can do all sorts of things, that some of the work about the smaller actors is neglected? How do you balance that?

Elizabeth Denham: In the investigation that I referred to in 2017-18 we were not just focused on the larger actors; we looked at the whole ecosystem. We took action against a small data broker, for example. We took action against a company called Cambridge Analytica, which was a very small company with a large amount of data. We had to seize 700 terabytes of data from that company. That company is no longer operating. You would think that is a small player, but the reach of that company's analytics was multijurisdictional. We are looking at large data brokers and smaller data brokers. The main political parties are not the subject of concern so much as the use of micro-targeting techniques that send our citizens down into a filter bubble, taking them out of the public square, to ensure that we can have free, fair and transparent elections.

As a society, this is such an important question, but the ICO can only do what we can do when it comes to personal data and the use of data to target individuals and serve them with certain content. The solution to this is really about the Electoral Commission and what it can do, the new content and conduct regulator — which of course is the subject of the White Paper — as well as the ICO. The solution to manipulation of voters is a team sport. It really needs more than just one regulator looking at these issues.

Lord Harris of Haringey: You said Cambridge Analytica was a small company with huge data. You then said that it is no longer in business. Does not that highlight the fact that a fining regime for what might be quite small ephemeral entities, in that they are set up for a particular purpose for a particular time and disappear, does not work? Do you need other powers to deal with, or to prevent, a small actor like that operating in that way and the individuals concerned carrying on as though nothing had happened?

Steve Wood: We are very aware that we need to be agile. In the last two to three years our approach to investigations has changed considerably. We have worked out that sometimes we need to follow the smaller players very quickly. We also need to have charts to follow where data goes to ensure we pinpoint the right points in the system as to where the harm is coming from. Because we have comprehensive powers, any organisation which is using personal data is what is called a controller, under data protection law. We can serve an information notice on any organisation in that situation to ensure that we get the information we need. Agility and moving very quickly are important in this space to ensure that people do not, as you say, collapse a company, move on, and it is hard to track them.

We have also been clear that we want stronger powers to be able to have director's liability, which we successfully argued for a few years ago. That enhances the case for accountability to be brought bear on individuals in certain circumstances, if it is appropriate.

Lord Harris of Haringey: You are comparatively small, yet you are dealing at the one end with some very large entities which can throw enormous resources at this and, at the other, the small agile actors that you are describing. What is the level of resource that you have? Is it anything like sufficient to deal with this?

Elizabeth Denham: We have considerably more resources than we had several years ago. We have approximately 730 FTEs working for the Information Commissioner's Office. We have been focusing on growing not just our numbers but our capacity and our effectiveness. We needed to bring in new skills. We have seconded economists and experts in artificial intelligence. We are working with the Oxford Internet Institute and the Alan Turing Institute on algorithmic auditing and transparency. I do not think we can ever grow the kind of public service that we will need to tackle some of these very wicked problems in digital society right now. We should also remember that some of the big tech companies may have thousands of engineers, designers and analytics experts, but we are the regulator with the power to compel information from them, with the power to be able to levy a stop processing order, which arguably interrupts their services much more than a fine.

The fines are of a level right now that they are not going to just be about the cost of doing business. There has been a significant uplift in the resources, the powers and the fees that support the ICO right now. Do we have enough? Probably not, but we have a significant uplift in the kind of capacity that we have to do forensic examination of data and to get the lawyers and the legal talent that we need. We also need to look at our litigation budget because that is where we could have a David and Goliath situation in terms of the litigation costs of taking on some of the larger players.

The Chair: Did not the litigation issue come up when we were debating your powers? I thought we managed to get rid of a ceiling for you.

Elizabeth Denham: We have been talking to government about our ability to retain some of our fines, because the fines right now go into general revenue. Retaining a proportion of the fines to be able to fund our external litigation costs is a conversation we are having right now with Treasury and DCMS. It is going to be really important because litigation costs could be pretty significant.

The Chair: And litigation costs are not absorbed automatically by the Government.

Elizabeth Denham: They are looking at it right now, yes.

Q292 **Lord Lucas:** How do you balance the need to deal with problems of the

here and now and devoting resources to planning and anticipating what problems might arise in the future? Do you have the support you need in both areas to do the job you think you should be doing?

Elizabeth Denham: I think you are referring to horizon scanning. It is really important for us to be able to look ahead and see what technology and what challenges are coming. Again, we have built some capacity to be able to do that. We have a technology panel of external experts to help us look at the horizon. We have expanded our management board so that there are more experts sitting around the table to help us look into the crystal ball. We have taken up the task of chairing the Global Privacy Assembly, which allows us to touch and get to know jurisdictions around the world and see how they are tackling the very same problems. One of the things that I am most proud of in the last 18 months is the work that we have done on the Age Appropriate Design Code, the kids' code. That is world-leading under UK law and I think it answers a lot of the concerns that the public have right now about keeping kids safe online and yet allowing them to benefit from all that the internet has to offer.

I know that my colleagues in the Global Privacy Assembly are watching this space very closely. Recently, we were in Silicon Valley talking to the technology companies and socialising them to our world-leading work. Our engineers talked to their engineers and we even talked to the Senate in California, which is very interested in a Bill that looks a lot like the Age Appropriate Design Code. We are quite proud of that work and we need to be connected globally because all these problems defy borders and parliamentarians and policymakers are concerned about the same issues.

Steve Wood: I can add a little more in the context of democracy and elections and how technology is going to affect it. Back in 2018 when we launched our *Democracy Disrupted?* report, we also commissioned a future-gazing piece of research from Demos and Jamie Bartlett, who is one of the leading experts in this area. We asked him to look five to 10 years into the future at what an election could look like. That gave us a picture about many more data points being available and potentially on sale in the market, which could be used for online targeting purposes, particularly thinking about the internet of things, and many more inferences about data that could be made to build up a much more granular picture of individuals. It also looked at things such as sentiment analysis and psychographics. This is still quite a nascent area and there is a debate about whether it works. It looked at the application of artificial intelligence to those areas. It is important we look ahead five or 10 years to what the risks will be and what the role of the regulator in this space. As the commissioner says, we are always getting the message about the importance of partnerships and working with other actors to tackle some of those challenges, because they are going to be really tricky.

Lord Scriven: You are painting quite a robust picture, which is good, but I think the Committee would like to hear about what is less robust. As you do this horizon scanning, what are the issues where either further work needs to be done by yourselves as regulators, or by government, to

make it more robust?

Elizabeth Denham: I mentioned the levelling of the playing field and bringing the other regulators up to a more modern place with modern powers. That is part of it. In terms of horizon scanning, I do not think we need to look very far out to know that the regulators cannot work in silos. If you think about the digital economy, competition issues are more and more reliant on data. Mergers and acquisitions are happening because of the data riches and treasures. We know that content and conduct regulation, which is the subject of the White Paper, needs new regulation, but that new regulation has to work really closely with us because data is what delivers the content, so it is the personalisation of the data that ends up delivering the content.

You can see that these siloed types of regulation are not going to work any more. One of the recommendations that we have made in response to the White Paper, and to this Committee in our written submission, is for a board or some kind of an entity which sits over the top of the regulators who are carrying out oversight in the digital economy. We think this is going to be really important. Again, all of us cannot land on the doorstep of a technology company with slightly different accountability mechanisms or slightly different audits we are looking at. There has to be a new way of regulating in the digital space. That takes some examination out into the future.

The White Paper was very focused on individual harms and not as focused on societal harms as we really need it to be. The Centre for Data Ethics and Innovation could play a stronger role in the kind of horizon scanning that we are talking about, so I would like to see that body more closely connected with the digital regulators, with those who oversee the economy, so that they are cracking on with the really challenging questions, not looking necessarily at micro-targeting because we have already looked at that. Can they not look three steps ahead? Connectivity between the Centre for Data Ethics and Innovation and Ofcom, the CMA, the ICO and the Electoral Commission makes a lot of sense.

The Chair: That makes total sense, but the problem is you are reporting into a Government who are themselves in silos. Our report will be of concern to at least three government departments and at the moment we are not quite sure which one of them takes the lead in this. Your oversight board is probably seen by government as being government, but within that you go back into deep silos. Do you have any possible solutions to that?

Elizabeth Denham: The Cabinet Office's work on democracy — so looking at imprints on ads and the provenance of ads and at political advertising — is being joined up with what the DCMS is thinking about. That is really important. BEIS is looking at similar issues. We just need a more joined-up approach. One thing the regulators are doing is meeting more regularly to talk about what is on our list and what we are doing. For example, we are a bit of a junior partner to the market study that the CMA is doing right now. It is looking at digital advertising and we are

investigating real-time bidding in the context of behavioural advertising. You can see how the regulators themselves are coming together. We could do more — as in the Government, Parliament and regulators — to get a handle on it. This is an issue that other jurisdictions are looking at. Australia, for example, is rejigging its regulatory scene to take account of the oversight of the digital economy.

Lord Lucas: Is there anything in the current regime which allows you to pick up on companies which use data subjects' information to disadvantage those data subjects without telling them specifically and obviously that their data can be used in this way?

Elizabeth Denham: There is a requirement in data protection around fairness. It is a relatively unexplored area of regulation. We are also starting to look at vulnerable populations and whether they are equipped to exercise their rights. That subject is of interest to us.

Steve Wood: One example we investigated a few years ago was the WhatsApp and Facebook case. It was about whether data sharing should take place between the WhatsApp platform and Facebook. Facebook had purchased WhatsApp many years previously and had indicated that data would not be shared between those platforms. However, there was an announcement that some form of data sharing would take place. We were very concerned about the imbalance there for consumers because their expectations had been set. What control would they have in that situation and would they really have a choice to stop using WhatsApp if their friends and family were using it? Ultimately, as the commissioner said, that would come down to a consideration and a judgment made on fairness. In the end, we resolved that case, and WhatsApp and Facebook signed an undertaking not to share that data further until full compliance with data protection law had been achieved. Those sorts of questions are going to come forward to us more and more over the coming years.

Elizabeth Denham: That is also where competition law, the competition regulator and the data protection regulator need to work together.

Lord German: May I pursue the idea of a board of regulators for a moment? I may be missing a page of your written evidence. Mine stops at paragraph 13 so it may be that I am missing more, but there is no mention of a board of regulators in the written evidence from your office that I have seen. It is a fascinating example of perhaps a new and critically useful idea. Could you give you some idea of how it would operate? Would it require a letter from the Government saying "This is how the boundaries would work"? Could you work it out yourself? Could you operate it now? You have just talked about AI and appointing staff to deal with that. The witness who came in just before you also talked about appointing AI people. Could you share staff? In what way could you co-operate without requiring necessarily the Government to take action and, even if they did take action, how would it work?

Elizabeth Denham: There would have to be some kind of governance structure. We would not want to create a whole bunch of bureaucracy

and slow things down. We would have to have some kind of agile relationship and agreement. One of the main benefits of us being more joined up in our work is that we could share expert resources and we could surge resources for large investigations that, let us say, the CMA is undertaking, where they need a lot of forensic experts, or some AI experts to be able to look at algorithm decision-making. We should not be competing against one another in fishing from the same pond. I would suggest that we have a shared resource of experts. It would be advantageous for those experts to work in a shared services arrangement because they could build their careers. What happens now is we have attracted some amazing technical staff, but the longevity of those same resources is usually pretty short because they are going to get pinched by somebody else. They get their experience in the regulatory field and back they go to the private sector. There are some advantages in us building a collaborative, co-operative regime to be able to tackle our issues about resources. If it is missing from our written evidence, it could be that I am remembering it from our response to the White Paper. I will get that to you.

Lord German: May I pursue that last point about collective responsibility? Could you organise it for yourselves as regulators, or do you require the Government to say to you, "You have to do this"? Where is the resistance coming in? You have given us what sounds to be a very suitable way of organising yourselves. Why not just do it?

Elizabeth Denham: We have quarterly meetings with the chief executive officers. We have a work programme that is happening at the official level. As I said, we are collaborating as a very junior partner on the market study which the CMA is doing. That is just the way we work together. If it was to be a more formal structure which shared the kind of resources that we were just talking about, that would need a lot of discussion with government. We are creatures of statute, we are independent and we need to carry out our independent statutory role, but we have to have a discussion about who is on first, whether it makes sense for Ofcom to go in as a content regulator and look at this issue, or whether it is more about data and therefore needs the data protection office.

Lord German: If you have a regulatory change in mind, do you have that written down somewhere so that we could have it as a bit of evidence?

Elizabeth Denham: We have floated the idea — I am corrected now — in our response to the *Online Harms* White Paper, so we can send that to you. It is not just our idea. It is being discussed with other regulators. Jurisdictions such as Canada or Australia are thinking about the same thing. They are thinking about joining things up because you cannot create a digital regulator which encompasses everything.

Lord German: Is there any other example of a board of the sort that you are thinking about anywhere else in the world at the moment?

Steve Wood: I am not aware of any. If we think of one afterwards, we will send the details to you.

Elizabeth Denham: There are some similarities in other areas of regulation that we could provide for you, even in the UK itself.

Steve Wood: Financial services is one area. It is a bit outside the sphere of what this Committee is considering, but we are also working very closely with the FCA on shared capacity. Also, for example, if there is a major cyber breach in a bank, that is of common interest to both the ICO and the FCA, so, again, we are exploring the shared capacity, but in a soft way. We are keen to evolve that to the maximum extent without impinging on our independence and decision-making and to see whether there is anything else we need to enhance to take it further. Independence is also always important for our role.

Elizabeth Denham: Independence is really important, but I think all the regulators have an appetite for getting things right for the public.

The Chair: We were impressed by the representative from Estonia, who made the point that to get the resources and everything else it needed, it seemed to be playing the security card as a sort of existential threat to them. Politics, in my experience, is a question of seizing the moment. Are there lessons we could learn right now from this COVID-19 crisis that we could apply and make it that much more possible to achieve the sort of coherence that you are suggesting?

Elizabeth Denham: It is a very good example of having the will and the appetite to tackle something such as disinformation in the context of a public health pandemic. We have seen the Government pull together the technology companies. We have seen the platforms working very hard to point users to official factual documentation and at least to make disinformation a lot harder to find. If you take the example of the pandemic, what I see there is a willingness on behalf of the platforms to design things differently and to make a move when there is a huge public interest to do it. It can be done. It is a matter of willingness to direct technical resources to do the right thing. Our Age Appropriate Design Code is an example of that. That is another area where it is about the willingness of companies to properly incentivise and to make their services work for children, and that is really important. We can learn something from disinformation in the context of the COVID-19 pandemic.

The Chair: I used to be president of UNICEF. I gave some information to colleagues over the weekend about disinformation being distributed falsely under the name of UNICEF, which was causing enormous problems. It has been quite difficult to get a lot of that material taken down. That is a good example of making a crisis work for us.

Q293 **Baroness Morris of Yardley:** You have already talked a little about working internationally with other organisations. Did you want to add anything to that in terms of best practice that we might learn? Particularly perhaps as Britain goes into a different relationship with the

EU, how do you think that might affect your work?

Elizabeth Denham: We are no longer sitting on the European Data Protection Board, but for the transition period of course we are still in the one-stop shop and under the envelope of work there. We are engaging with many jurisdictions around the world, including through our chairmanship of the Global Privacy Assembly. We are aware of different practices on this topic of data and democracy. When we look at what the Japanese do, they just do not allow political advertising at all. We look at Finland and Estonia as examples of doing very good things to be able to control disinformation. We look at Australia and Canada and their work with the G7 and the G20 on ethical data uses and extending the powers of regulators to cover political parties. We are learning a lot from the rest of the world. We certainly do not have all the answers, but it is very positive that we can look around the world. We are also a law enforcement agency, so we work closely with the Federal Trade Commission in the US on anti-spam or anti-marketing enforcement structures, so we have some experience there.

Steve Wood: It is very important to look at how different platforms are being used in different ways in different countries. Certainly, we have observed in countries such as India and Brazil that WhatsApp is a key campaigning platform. In the last election in the UK it was less so, but I am reading articles saying that WhatsApp may play more of a role in the US presidential election this year. We want to be learning to see how platforms and different trends may emerge in the UK, because it helps us learn how we can work with other regulators which have perhaps taken steps to tackle some of those risks. The international side to our work is always important for what we learn about different risks and how those challenges can be tackled through different solutions.

Baroness Morris of Yardley: It sounds as though the structures are there for you to do that. Could you say a bit more about the EU situation? You talked about no longer sitting on the organisation, so how will you fill that gap next year?

Steve Wood: The UK became an independent country when we left the EU at the end of January. That means the ICO does not have a seat at the European Data Protection Board. During the transitional period, EU law still applies, so we are still following EU law, which is the GDPR. At the ICO we have had an international strategy since 2017 to think about where else we need stronger links as a regulator in the world. We want strong links with the EU after we have exited, and we need to think about where else we need to link up with. We know these challenges are global in any case. We are also taking more of a role in the OECD. I am chairing the OECD's working party on data governance and privacy. There are a number of big issues there about children online, et cetera, and how those sorts of recommendations coming from a global body like the OECD can influence.

The UK has a number of different places where it can still engage and bring its influence to bear. Clearly, as we move away from the European

Data Protection Board, we will still have very close links with our European colleagues. The key one to mention is Ireland. We are still part of what is called the one-stop shop system for all cross-border cases in the EU until the end of this year as part of the transitional period. Some of the big issues about the transparency of the big online platforms are with the Irish Data Protection Commissioner at the moment. That regulator will make some very big adjudications this year and we are watching that very closely. We fed into them because we are what is called a concerned authority; Ireland is the lead authority under the EU system. That includes matters that we have referred about targeting adverts using sensitive categories of data, for example. There are some important issues there and we are always going to have a very strong relationship with that regulator as well. It is a matter of identifying who those key players are to ensure we can always act quickly. If we have the partners, we can often refer matters to them and they can take action in their jurisdiction, when it may be difficult for us to take cross-border action for reasons of territorial scope, et cetera.

The Chair: Now that we have effectively withdrawn from the EU, have you detected any lessening of enthusiasm in the UK Government for GDPR?

Steve Wood: The message from the Government is a commitment to high standards. That was the message the Prime Minister set out in his key statement where he outlined the UK's approach to having independent policies. One of those areas was data protection. We still recognise that message of high standards of data protection as being the key approach. The UK also wants what is called an adequacy agreement, which is recognition by the EU of the UK's data protection law as being, essentially, equivalent to EU law so that data can flow from the EU to the UK. That is another important process which is ongoing alongside trade discussions. It is a technical decision the EU wants to make.

Around the world, standards are going up. That is the key message. India is just about to pass a law; that is the largest democracy in the world. Brazil's law comes into force this year. There is a new law in California. All around the world there is a convergence of global standards, so I think the UK must always look at that position in terms of why high standards are important for trust in the digital economy and growth and all those sorts of issues.

The Chair: Can we as a Committee assume that the high standards are GDPR plus or GDPR minus?

Elizabeth Denham: I do not think it is about GDPR. It is about the strength of the principles in the law. I would not say that our office has any GDPR zealotry, but I think the principles in the law are really important. What the GDPR did, and this is not widely known, is it looked at the best practices around the world — from the US, Canada, New Zealand, Australia and Europe — and took the best of breed and put them in that law. It is not the detail in the law. The law represents the best practices from around the world. A lot of those practices came from

UK law because of course we have had data protection law since 1984. This country has a very long tradition of high standards of data protection and yet pragmatic, proportionate administration of the law, and I think that is what the UK stands for.

The Chair: I am not torturing this matter, but it occurs to me that the US has real reservations about GDPR and about the notion it goes too far. I have had people say to me — because I sit on this Committee — that they feel we have tended to interpret GDPR at its extreme end. I am concerned, and it is a legitimate concern for us as a Committee, as to whether there is any backsliding taking place here towards a US position.

Elizabeth Denham: I think the US position is changing. Let us look at what is happening at state level in California, Maine and Florida, for example. Washington had a Bill and is going to come back with another Bill. As Steve said, standards are going up around the world. When it comes to the GDPR, US companies have made adjustments to it because they are subject to the laws for services that target EU residents. That is an issue around the world. When it comes to our office, one of the myths that I would like to bust is that we are at the extreme end of enforcement, when, in fact, probably 75 per cent of the resources in my office are put to assisting and helping. We have a small business enterprise stream of work. We gave half a million pieces of advice on our helpline last year. We review and give advice to government and to Parliament. We are helpful. When we use the extreme end of our powers, it is because it is an action of last resort. In a sense, when I see a fine, it is a failure of the system. It is not what we want to do. Much more of our work is directed at guidance, guidelines, education, training and helpfulness. We are the friendly neighbourhood regulators. I want to bust the myth that we are otherwise.

The Chair: Quite right too. I think Baroness Kidron has an interest to declare.

Baroness Kidron: I need to declare that I was one of a number of people who brought the Age Appropriate Design Code into legislation in this House.

My question builds on what you have just said, which is data protection is often characterised as being anti-innovation. Could you say something about attitudes both at the SME level and at the platform level? What is your experience of engaging with them? Is there is an innovative piece to this?

Elizabeth Denham: By law, we are required to take account of innovation in our decisions and our work. That is in the statute and in our mandate. Since 2016 we have been very focused on innovation. I would say we have been laser-focused on innovation. We are the first data protection authority in the world to run a sandbox. A sandbox is where companies and innovators can come and beta-test their new services. These services are pushing on the boundaries of data protection. In our sandbox right now we have large players, public sector players such as

the NHS and small innovators, and we are giving them the specialised advice to be able to bring their services to market.

We received a grant from the Regulators' Pioneer Fund which allowed us to build a platform to help other regulators understand data protection. We have hired a new deputy who is charged with innovation. That is Simon McDougall's job description. A couple of weeks ago, we went to Silicon Valley before all the flights were grounded. The reason that we went there is we wanted to meet the companies and have our engineers talk with their engineers to be able to test the Age Appropriate Design Code and get ready for the one-year transition period. We can run text sprints and we can give guidance to the private sector on how they can comply with it, but we are very much focused on innovation. We have a team of technologists and engineers that are there to help. I mentioned earlier our AI auditing tool and our explainability tool. Again, that is about innovation with trust. It is a focus of what we do.

Baroness Kidron: I have noted that a number of my colleagues have raised the question of resources. Does the sandbox or this part of it need more resource, more capacity and more scale, if we are going to see a different world where people understand all these issues?

Elizabeth Denham: I think that is right, because we had 70 or so applications for our sandbox and we are only able to service about a dozen of them. You can see there is a capacity challenge there, but to do that work, we need to second experts from large consulting companies and technology companies. Yes, there is an appetite for more sandbox, but, again, we are testing our ability to do it right, and this takes several years. We will have a report out by the summer on how the first year of sandbox has gone.

Q294 **Baroness McGregor-Smith:** Moving to the evidence submitted that you will have seen from the Conservatives, Labour and the Lib Dems, do their claims match your assessment of how they conduct online campaigning? Were you particularly surprised by anything?

Steve Wood: In terms of the evidence they submitted, it is characterised by how they approach political campaigning. The key message we get from the political parties is they are taking the issue of data protection seriously. The larger parties, with the resources, are appointing people who are responsible for data protection and have also considered the issues which we put out several years ago on the importance of very carefully considering the fairness of using larger datasets and about using different techniques in political campaigning. The points that they have made there align with what we have learned from the previous auditing of the political parties.

It is an ongoing conversation with the political parties to understand the ways they want to use data, and for us to approach it in an objective manner, as I said earlier. Data can be beneficial to democracy. We understand, as I said earlier as well, that the political parties have the spine of the electoral register. They have the dataset of the entire UK

adult population. They will want to learn more about voters to interact with them. However, it is important we work with them and provide them with the right guidance to illustrate how they must do that within the law. Clearly, the more data you have, or perhaps the more intrusive the algorithms become, and the greater the profiling and categorisation, the greater the risks. That is where we need to provide the guidance to the parties to help them get that right. It is always going to be done by focusing on what is good for democracy. We need to guard against the risks of misuse of data but, equally, recognise that as a regulator in this space we need to enable fair use of data, because data can help political parties understand the electorate as well.

Baroness McGregor-Smith: I understand your role in it, but what do you think the public think your role in all this is? You are obviously working and you have a view: what do you think the public think you do?

Steve Wood: The public's awareness of this issue is a good question and we looked at it when did our *Democracy Disrupted?* report in 2018. It is quite challenging as regards transparency and awareness of the public. The public probably have some notion that the political parties have some information about them because they get letters through the door still, and they may see some political ads online, but they do not understand how the whole ecosystem works. Initially, when we did our investigation, we looked at 30 organisations. We called it "pulling back the curtain", to show the public this is how data can be used in political campaigning, and we want this to happen in a safe, fair and proportionate way. Transparency is challenging in this area because you are talking about the whole adult population. How do you get information out? It is not just one company reaching its customers. It is a challenging issue.

We have also spoken to the Electoral Commission about ensuring there is better information on registration forms. This is not to scare the public and not to try to warn them about uses of data, but just to make them aware that the political parties have the right to have the core dataset—the electoral register—so they have some awareness of that spine as well. We get a significant number of a complaints about address mailings. However, they are within the law because political parties are allowed to send one of those during a political campaigning position. We need to work more closely with the Electoral Commission on the issue to try to raise awareness. It is probably going to be an ongoing task. We are also happy to work with the Cabinet Office to see what else can be done.

The Chair: There is a question from the ether from Lord Mitchell, who is watching. He makes the point that as a Committee our experience with the political parties is somewhat different from yours. With the notable exception of the Liberal Democrats, we have had very little co-operation indeed. Worse than that, we have competing claims as to whether the Labour Party did or did not purchase data. We really have, in a sense, failed to engage with them, and it has been a source of frustration, but your experience has been somewhat different. Is that correct?

Steve Wood: We have had a degree of co-operation right the way through the process with the political parties. It is ongoing and we need to continue to do that.

Elizabeth Denham: What is important is that their compliance with the law is understood clearly. Again, we want to level the playing field. It should not be the party with the biggest budget which can reach the electorate. There is an issue of fairness there and there is such a connection between funding political campaigning and data use because, as we know, data is collected 365 days a year and not just during the regulated period. That is why we need to work together, but the parties have been co-operative. One of the bigger concerns I have is with the technology platforms, because their response to political advertising has been idiosyncratic. We have seen ad libraries, some that work, some that do not. We have seen some platforms decide that they are going to ban political advertising. We see others taking other measures and in this space we really want to drill down on what is fair and how data should be used. That is really what we are trying to do.

The Chair: Baroness Morris offered some evidence of the fact that certain political parties believe it is legitimate to seek an edge, irrespective of whether that edge is wholly legal or not. That is a very real concern for us, and I am sure it is something we will address. There is a supplementary from Lord Lucas.

Lord Lucas: What document best sets out your views on how the principle of fairness should apply in these circumstances? Just as an aside to that, will your audit of the parliamentary parties be out before we have to go to press on this report or will we not have that advantage?

Elizabeth Denham: Our audit of political parties is a couple of months away before it is published. I am not sure what the deadline is for this Committee on the publication of your report. Our *Democracy Disrupted?* report from 2018 has a lot of detail in it which you might find helpful. The Electoral Commission has done some work, and I think there are other reports around the world that we can point you to, Lord Lucas, that would be helpful to answer your question.

Steve Wood: We can also send you some more links to guidance we already have on our website about fairness. That particularly encapsulates the concept of reasonable expectations, ensuring you always look at fairness from the perspective of the public, and we can provide some more information about that as well.

Elizabeth Denham: To add to the question that you asked earlier about how we know what the public think about us, we ran some focus groups with the public in the context of our *Democracy Disrupted?* report. There is some reporting out of our focus groups in that report as well.

Lord Scriven: This subject has a real rub and there is a tension. From your perspective, is this an issue purely about compliance for the political parties, or is there anything you have seen from your international work

which could be useful and go beyond compliance to make it even better practice? That is the real rub and the real issue around this question.

Elizabeth Denham: There is a piece of research that we commissioned for the Global Privacy Assembly about international practices and data and democracy. That was undertaken by Professor Colin Bennett and it might be useful for us to share that research with you. The challenge is that jurisdictions have different cultural attitudes towards politics and political parties so it is not one size fits all, but we will send you the research that Professor Colin Bennett did on this.

Lord Scriven: May I push it because we are not going to get you in the seat again? Even with the cultural differences, et cetera, is there anything you would see as the commissioner which would be helpful beyond compliance in a UK context?

Elizabeth Denham: Our guidance on the use of data in political campaigns is helpful because it is the result of wide consultation and it is not just about the UK. That guidance really takes the law, including the democratic engagement exemption, and explains it in a clear way. May I point you to that as well?

Lord Scriven: It is predominantly about compliance. Is that what you are saying? I am sorry to push you on this, but I need to be clear, because it is a big question and a big issue the Committee is dealing with.

Steve Wood: Another good way to look at it is that there is a requirement in data protection law under the GDPR, when organisations are undertaking processing and uses of data which start to indicate certain elements of risk, for a data protection impact assessment to be undertaken. It is very important that all actors in the ecosystem are using data protection impact assessments. To go to your point, Chair, about parties or other actors trying to get the edge, particularly by buying in data or doing different activities with data, they should be using that as a tool. Also, it is an ethical tool and you can have an ethical impact assessment linked to that, which takes quite a rounded view, and takes it from the view of the citizen as to what the public would expect in the situation. It enables organisations to work it through from a number of perspectives. I guess it is an example where it is a requirement of the law but, equally, you can use a data protection impact assessment to go that bit further to draw out what we should do in that situation.

Elizabeth Denham: To get it best practice.

Q295 **The Chair:** I have a question which has come up time and time again, and that is to do with the relationship between the social media companies and researchers, and the ability for researchers to do the job that they feel they could do to support and help us all. What work has the ICO done to consider how researchers can best access data from technology companies without breaking data protection laws? Do you think that privacy laws are a barrier to data sharing for research

purposes, as has been suggested to us by Facebook? It is a cause of enormous frustration in the research community.

Steve Wood: The first, straight answer to the question is data protection laws should not be a barrier to data sharing for research purposes. It depends on the context, nature and the type of data. We have not had a specific conversation with the technology companies about this issue yet, but we are happy to. It is about recognising the legitimate public interest in these types of research being undertaken. It is about working with some groups of experts to understand what different techniques could be deployed to minimise the privacy risk. If these datasets contain personal information, there is some risk that individuals can be identified, but if they can be effectively anonymised and the risks removed, the researchers can interact and use the datasets in a particular way. We would need to understand more about the types of data the researchers require.

The overarching answer is we would want that research to take place if it can be done safely and effectively. There are many different ways that research can be approached and different ways the data can be sliced to make it safe and fair. If you are taking users' data off the platform, that could be a question for data protection law, but it is not a question of saying no. It is question of working through it again and talking about an impact assessment. That would be our answer. As an organisation, we are very supportive of public interest research and data protection not being a barrier.

Another statutory code we have had since 2011 is our data-sharing code. We are just about to update and publish that later this year. That provides lots of guidance for all organisations on how data can be shared in the public interest because it is important for societal reasons. It is a myth we have to bust. Often, people think it is quite difficult to work through the issues, but we want to provide practical guidance to give people the confidence to be able to do those things in the public interest. We have had not had a direct conversation, but we are happy to take it away and think about it.

The Chair: May I suggest that you use the COVID-19 crisis? It is a classic example of inadequate data possibly preventing us coming up with solutions which would solve problems that at the moment we do not have any idea how to solve. This is a personal view. The excuses that we have heard from the social media companies just do not stack up, because what they are really illustrating is a complete lack of trust. If trust does not exist between the research community and the people it is supposed to be working with, you have a pretty dismal situation.

Elizabeth Denham: I agree, Chair. One of the really big issues is around transparency. What do we mean by wanting more transparency from the platforms on what kind of data and requests they have, and how quickly they take data down and how they deal with disinformation? We need standard practices and processes, and those need to be reported on, so

that we can get away from this idiosyncratic approach to data and the use of data on platforms. The current crisis is a great case study for that.

Steve Wood: In the COVID-19 example we are also learning about how data sharing probably needs to be improved around location data for mobiles, because that can be used to trace epidemics. There has been some really good work done and we are trying to enable that to be done safely because we can see the value it can have.

Q296 **The Chair:** It is a fantastic moment for us, in a way. The last question is: if the Government could do one thing to better support your work, what in your view, jointly or severally, would it be?

Elizabeth Denham: I am going to go back to the innovation point. As you know, we have a great appetite to support innovation. If the Government can continue the Regulators' Pioneer Fund so that we can access some funds to do the right thing, that would be really helpful. It is about supporting innovation by regulators in regulatory practice. That is a great example of what the Government can do. The Government might be able to help us bust some of the myths that the ICO is just about the pointy end of the enforcement stick. Part of the work that we are doing right now in the context of the pandemic is getting us there. We have put out some guidance about regulatory forbearance in the context of the COVID-19 crisis and Q&As for the public, clinicians and others who need to gather data, and gather it quickly.

The Chair: Steve, do you want to add anything?

Steve Wood: No, that is fine.

The Chair: You get the Bible and the works of Shakespeare. Thank you both very much indeed. It has been a hugely useful session for us.