HOUSE OF COMMONS

Digital, Culture, Media and Sport Committee

Sub-Committee on Online Harms and Disinformation

Oral evidence: Online harms and the ethics of data, HC 646

Tuesday 26 January 2021

Ordered by the House of Commons to be published on 26 January 2021.

Watch the meeting

Members present: Julian Knight (Chair); Kevin Brennan; Alex Davies-Jones; Clive Efford; Julie Elliott; Damian Green; Damian Hinds; John Nicolson; Giles Watling; Mrs Heather Wheeler.

Questions 236 - 354

Witnesses

I: Elizabeth Denham CBE, Information Commissioner; and Paul Arnold, Deputy Chief Executive and Chief Operating Officer, Information Commissioner's Office.

Examination of Witnesses

Witnesses: Elizabeth Denham CBE and Paul Arnold.

Q236 **Chair:** This is the Digital, Culture, Media and Sports Select Committee and a meeting of our sub-Committee on disinformation and fake news. Today we are joined by Elizabeth Denham, the Information Commissioner, and Paul Arnold, deputy CEO and chief operating officer at the Information Commissioner's Office.

Before we begin I will just check with members to see if there are any interests to declare. No, a lot of shaking heads. Brilliant.

Good morning, Elizabeth. Good morning, Paul. Thank you for joining us.

Elizabeth Denham: Thank you for the invitation and the opportunity to account for the work of my office.

Q237 **Kevin Brennan:** Good morning to both our witnesses. Elizabeth, could you briefly tell us—as we haven't seen you for quite a long time—what you feel you have accomplished in your office? Do you have any loose ends or any unfinished business that you wish you had accomplished while you served your term of office?

Elizabeth Denham: The ICO has been on a journey in the past four years and we have had the challenge of bringing in a new law, the Data Protection Act 2018. We have had the challenge of Brexit, the transition period, and we also have the challenge, like everyone else, of the global pandemic. It has not been a smooth ride for the ICO.

What I am most proud of is that my team and I have been able to build the capacity and the capability to be able to respond to issues that are larger than life and are certainly of concern to your constituents, to Parliament and to Government. Back in the day, even three or four years ago, if you said you were a data protection commissioner that might be a conversation stopper at a party, but now I think data protection is mainstream and it sits at the intersection of law, technology and society.

We have had the capacity to grapple with issues such as the use of data in political campaigns, we have grappled with children's rights online. We have responsibilities for regulating in the digital economy, and now we are involved in being an expert adviser to Government on trade deals.

Q238 **Kevin Brennan:** I want to ask you a few questions about one of those issues to get it out of the way. You kindly wrote to us in October concerning the whole investigation the predecessor Committee was doing into Cambridge Analytica. In August last year the US Senate Intelligence Committee published a report and late on in that report—and I confess I have not read it all because this is on page 664—it says, "Finally, the Committee was unable to obtain the corporate communications of Cambridge Analytica or SCL Group, which had already been seized by the UK authorities." Did the Senate Intelligence Committee contact you and ask to see the evidence? How did you respond if they did?

Elizabeth Denham: The committee did not contact my office to ask for the evidence that we had seized from the servers of Cambridge Analytica.

Q239 **Kevin Brennan:** What would happen if they were to do so now?

Elizabeth Denham: If there was a proper request for information, we would certainly share that information. We shared Cambridge Analytica data and analysis with the Federal Trade Commission in the US, for example. Also, we have shared information with state Attorneys General who were carrying out their investigations, and with the Securities and Exchange Commission.

We have the ability in our law to share information if it is necessary for another law enforcement agency.

Q240 **Kevin Brennan:** On that point, are you able to supply us with a list of the countries and agencies that you have assisted throughout the duration of your inquiry into this?

Elizabeth Denham: I can provide you with that information. I would like to write to you after this session to give you a full list of the various data protection authorities around the world that we have shared information with.

Q241 **Kevin Brennan:** In April 2019 your office had originally committed to produce a final report into the seizure of the servers that your office carried out. That never arrived, but a year later you wrote the letter, which I referred to earlier, rather than producing a final report for the Committee. What was the reason for the delay, and why didn't we get a full report? Why did we get a letter instead?

Elizabeth Denham: The letter was extensive, as you will know. My office produced three reports on the investigation into the misuse of data in political campaigns. We had a policy report and two enforcement reports. We had looked at the entire ecosystem of data sharing in campaigning.

So beyond Facebook and Cambridge Analytica, we also investigated and audited political parties, and we audited data brokers and credit reporting agencies. The strands of that investigation are, in my view, reported out sufficiently in all our work. The letter was our final line on the report. Taken together with the policy and the enforcement actions, prosecutions, fines, stop-processing orders, we had done a lot of work in this space. What is important here is that we pulled back the curtain on the use of data in democracy, which has been taken up by many organisations and parliamentarians around the world. It was the exposure of a systemic issue.

Q242 **Kevin Brennan:** I am not quite sure why that could not have been issued as a report but, anyway, what happened to material that fell outside of the remit of the investigation but was not passed on to other agencies?

Elizabeth Denham: For clarity, are you talking about information that didn't relate to algorithms, data or data protection?

Kevin Brennan: Yes, I understand some material fell outside the remit of your investigation or your legal powers and some of that got passed on to the National Crime Agency and so on, but there was other material that was not passed on to other agencies. What would have happened to that material?

Elizabeth Denham: We have the material. Our office has the material and we are going through the process of determining what is best done with the terabytes of data that we seized from Cambridge Analytica. When there were issues that were beyond the mandate of my office, we have passed on information to the National Crime Agency, the National Cyber Security Centre and so on.

It is my job to regulate data, not to regulate potential criminal activities. Our sharing of information involves the Insolvency Service, so we passed on information from Cambridge Analytica to the Insolvency Service for them to determine whether or not they were going to take actions against any of the directors of Cambridge Analytica. They did, and they struck Alexander Nix from the register so he is unable to be a director. That is beyond my office.

Q243 **Kevin Brennan:** Okay, but what you are saying is that you still have the material that did not get passed on. What will happen to it?

Elizabeth Denham: We are determining what should be retained and what can be properly disposed of. We are in consultation with other experts on this.

Q244 **Kevin Brennan:** Some information has come to light subsequent to the letter you sent to the Committee in October. In particular Brittany Kaiser published some further evidence that seemed potentially to undermine the idea that Cambridge Analytica and AIQ's relationship was not much closer than suggested in your letter, that in fact it was a contractual partnership. The Canadian Privacy Commissioner in their report also said categorically that AIQ made use of SCL Cambridge Analytica datasets and did so illegally. Do you accept that is further evidence that perhaps the two companies had a much closer contractual relationship than you suggested in your letter? I suppose your letter, if you like, denied that relationship. It did not supply the underlying analysis we might have got from a report. Is further analysis of why you came to that conclusion something you can provide to the Committee?

Elizabeth Denham: I certainly can offer a private briefing to the Committee to unpack that finding. I am certainly willing to do that. The difficulty of this investigation is that there were so many commentators in the public sphere. We are a regulator, and we have to be driven by the evidence that we find. I believe that we have done that to the extent of our abilities, our powers, and if there are commentaries and commentators that feel differently, they have the opportunity to come

forward and provide us with the information. I have to follow the evidence, I have to balance and weigh the evidence and come to the conclusion that we did. Although there was some UK data in the hands of AIQ, we did not find that there was a close relationship at the time, in terms of the referendum, between AIQ and Cambridge Analytica.

Q245 **Kevin Brennan:** Do you think the further evidence that Brittany Kaiser supplied has any relevance?

Elizabeth Denham: It could possibly have relevance but, again, as a regulator we have to follow the evidence and we have to be able to question witnesses and the statements that they provide.

Q246 **Kevin Brennan:** Are you confident at this point that the evidence or the data that you are destroying is not premature? Might it be sensible just to hold on to some of it for a bit longer?

Elizabeth Denham: We have not said that we are destroying it at this time. Again, I can offer a briefing for any members of the Committee to be able to go through the detail of what our considerations would be. I would underscore how significant this investigation was, because it was the first time that a data protection regulator had to go into the depth of forensic analysis with the huge amount of data that we seized and the witnesses that came forward. We needed to see the evidence, not just the lines that they are taking to make a public commentary. We have to be evidence led.

Q247 **Kevin Brennan:** A couple more questions on this. I know we have a bit more time this morning. In 2018 Mark Zuckerberg testified before the US Senate Commerce, Science and Transportation Committee, and he promised that Facebook would conduct a full audit of Cambridge Analytica's servers after the UK Government completed their investigation. I think he meant you. In your letter you also state that you are in the process of returning materials to SCL Cambridge Analytica's administrators or destroying material. After your October 2020 letter and the completion of your investigation, did Facebook contact you to complete their audit?

Elizabeth Denham: Once again, I think I could answer that question with you and the Committee in private.

Q248 **Kevin Brennan:** Isn't it a fairly straightforward thing to ask, whether or not they contacted you about completing their audit? After all it was a commitment that Mark Zuckerberg gave in the public domain before a US Senate Committee.

Elizabeth Denham: It is part of an agreement that we struck with Facebook in terms of our litigation against Facebook. There is an agreement that is not in the public domain, and that is why we would prefer to discuss this in private.

Q249 **Kevin Brennan:** Have you kept all documents, emails and data that

might be of assistance to other countries or jurisdictions in their investigations, because there are others going on around the world?

Elizabeth Denham: We have.

Q250 **Kevin Brennan:** Finally, and I won't overindulge on this, you mentioned your reports about political parties in your earlier answers. In that letter to us in October you said, "We will shortly be publishing the reports of the findings of our audits of the main political parties, the main credit reference agencies and the major data brokers as well as Cambridge University Psychometrics Centre. We will write separately to the Committee on those issues." When do you plan to provide that information to the Committee?

Elizabeth Denham: We have published the audits of the political parties. That is done. We have also published the result of our investigation into the credit reporting agencies, including an enforcement notice against Experian. We are soon to publish our investigation into data brokers and, in the next few weeks, we will be publishing our guidance for political campaigns and their use of data.

Q251 **Kevin Brennan:** Moving on to a slightly different area briefly, when did you become aware of WhatsApp changing its terms and conditions, which happened recently, to allow sharing of information with Facebook? Are you concerned about the way big corporations do this? Are consumers really getting a choice when a platform does this sort of thing?

Elizabeth Denham: What is very interesting about the WhatsApp announcement of ongoing sharing with Facebook is how many users voted with their virtual feet and left the platform to take up membership with Telegram or Signal, which use end-to-end encryption.

Q252 **Kevin Brennan:** How many did that? Do you have any figures for us?

Elizabeth Denham: Millions. I can get the specifics, but I read about this in probably the same way that you did, I read about the change in the terms of service in the media. However, you will note that the change in the terms of service and the requirement of users to share information with Facebook does not apply to UK users or to users in the EU. That is because in 2017 my office negotiated with WhatsApp so that they agreed not to share user information and contact information until they could show that they comply with GDPR.

Q253 **Kevin Brennan:** So you are telling us that all those people changed their service needlessly because it did not apply to them?

Elizabeth Denham: That has been reported extensively but, at the same time, I think it is a bigger issue of trust. Users expect companies to maintain their trust and not to suddenly change the contract that they have with the users. It is an example of users being concerned about the trustworthiness and the sustainability of the promises that are made to them.

Q254 **Kevin Brennan:** Do you think these big, huge, powerful corporations should be able to buy up smaller operations just to exploit their users, who start with very different expectations of what they are getting into and are then almost trapped into using those services, although in some instances there is a real opportunity to change? Why should they have to change if they have signed up to a particular regime they thought they were getting into? In any case, as we all know, a lot of businesses exploit the natural inertia of people who simply do not have the time, or the opportunity costs are too great, to get involved in changing all their data services. Isn't there a real gap in the law in allowing this sort of thing to happen?

Elizabeth Denham: Competition authorities are looking at mergers and acquisitions with new eyes. Mergers and acquisitions that are, at their heart, about seizing and controlling more personal data is a real issue. You will see that the Competition and Markets Authority in the UK is looking at this issue quite closely. Our office, the data protection authority, is working with the CMA on issues of personal data, the target of which is important for companies that are merging.

What you are asking is, is this fair and, as policymakers, regulators and civil society, do we need to see changes in the way big tech is regulated. The answer to that is absolutely yes.

Data is such an asset in the digital economy that we need to look afresh at how data and competition work in the digital economy. Content and conduct regulation is the focus of the Government in its online harms legislation.

Q255 **Kevin Brennan:** Do you personally use WhatsApp and Facebook?

Elizabeth Denham: I do not. I am not on WhatsApp—I do use end-to-end encryption messaging—and I am not on Facebook. My choice.

Q256 **Kevin Brennan:** Which service do you use for end-to-end encryption messaging?

Elizabeth Denham: Signal, for my personal communications.

Kevin Brennan: Thank you, Elizabeth.

Q257 **Chair:** Just to clarify the relationship between WhatsApp and Facebook on data, Niamh Sweeney appeared before the Home Affairs Select Committee last week and we had an exchange there. I am just going to read you what she said to me. I just want to make sure this is correct and this is the case, if that is okay. She stated, "There are no changes arising from this update to our data sharing practices with Facebook anywhere in the world, especially the UK." Is that correct?

Elizabeth Denham: What I have read in tech journals is that there are changes in terms of sharing information with Facebook, particularly contact information and the contact information of users' friends. That is my understanding from reading detailed tech reports in the public

domain. But, again, it is an important question to ask of the company in a regulatory call or regulatory review.

Q258 **Chair:** Are you going to do that?

Elizabeth Denham: I will do. Again, we received an undertaking from WhatsApp not to share information with Facebook, and that goes back to 2017. That applies to UK users, and my understanding is it also applies to EU users.

Q259 **Chair:** As with GDPR?

Elizabeth Denham: Yes.

Q260 **Chair:** That is an undertaking from 2017. Have you asked for a specific undertaking at this point in time?

Elizabeth Denham: No, because up until 1 January it was the Irish data protection authority's job to oversee the activities of WhatsApp. So as long as we were in the transition period, the one-stop shop meant it was my Irish colleague who was responsible for WhatsApp. That has changed now.

Q261 **Chair:** How long will it be before you can produce for the Committee the answers from Facebook and WhatsApp on whether or not there is any sharing of data between those two platforms?

Elizabeth Denham: I will follow it up, and I will respond to the Committee.

Q262 **Mrs Heather Wheeler:** Good morning to both of you, very kind of you to come along. The beauty of these meetings is you didn't have to go out in the snow. Well done, nice and safe.

I am interested in a couple of different areas. The first set of questions is about the Freedom of Information Act. Straightforwardly, do you still consider that the current Freedom of Information Act is fit for purpose, or is it not fit for purpose?

Elizabeth Denham: We used to answer questions about the transparency agenda and freedom of information. When I was at my scrutiny hearing in 2016, I think the DCMS Committee got the impression that I was fundamentally an FOI advocate. A lot of the work I had done in Canada before coming to the UK was focused on fairness, transparency and openness in Government. When I came to the UK in 2016, Lord Burns had done an independent study on whether or not the FOI Act was fit for purpose.

His conclusion, and his Committee's conclusion and report, was that the FOI Act worked relatively well, with some recommendations for improvements. My main parliamentary report on transparency was issued in 2018, and that report was about the need to extend the FOI Act to cover the delivery of services by the private sector. What is needed to

make the Act work in a way that is fair to the public is that the Act needs to reflect how public services are delivered.

The pandemic has only accelerated the range of actors involved in the delivery of public services. The same accountability should apply to the private sector that is delivering fundamental public services.

Q263 **Mrs Heather Wheeler:** To be clear, do you think that the right to information should be extended to all organisations that deliver Government services?

Elizabeth Denham: I do.

Q264 **Mrs Heather Wheeler:** That is absolutely fascinating. The obvious next question is, who should bear the burden of costs associated with those freedom of information requests?

Elizabeth Denham: Fundamentally, what is important is that citizens have a right to hold organisations to account, to understand how decisions are made. If you take a housing association that falls outside the Act, an individual does not have the right to access information about the safety of their housing. I do not think that is fair.

Who bears the burden of costs? Obviously private sector companies that are delivering service under massive contracts could bear the burden of those costs. Again, how this would work in practice, in extending the reach of the Act to cover private sector delivery, you could come up with a threshold of the value of the contract before that organisation is subject to transparency requirements.

Q265 **Mrs Heather Wheeler:** That is very interesting, thank you for that. I am now going to go off on a slightly different tangent, but it is something we have already talked about this morning.

I am interested in GDPR, because I have such a technical understanding of it all, obviously. What have been the biggest problems for the ICO in moving to GDPR? Paul, I don't know if this is something that might be more up your street, but if Elizabeth wants to carry on talking that is fine. Whoever wants to take it.

Elizabeth Denham: I am happy to have Paul speak to that. The reason it is appropriate for Paul to address this is because the change the ICO had to go through to bring in the Act, to administer the Act, was under his mandate and his function at the ICO.

Paul Arnold: As the Commissioner says, the mandate that changed for the ICO in 2018 was something we were preparing for in the build-up, as you would expect. I would probably categorise it in three ways. There was a fundamental capacity challenge for us, a capability challenge and then the all-important culture of the organisation.

If I talk about capacity first. There was a pretty immediate and profound increase in demand for all ICO services from May 2018 onwards. Most of

our historical and traditional services simply exploded in demand with something like a 130% increase almost overnight. The new duties that came with DPA 18, particularly the ones for us to have due regard for economic growth, also saw it introduce a number of new services, which in and of themselves brought their own demand to our door. We had a really basic capacity challenge from 2018 onwards to meet what was effectively about a 150% increase in demand for our work.

Since 2017 we have increased the size of the ICO by about 85%, so we now have an FTE workforce of just over 750. We have done that in a very deliberate, precise and responsible way, as you would hopefully expect, making sure that we were unlocking efficiency and productivity as we moved forward. It was an essential and very rapid requirement for us to scale up our services overnight.

In terms of the capability of the organisation, that is something all regulators obviously do on a rolling basis to assess what skills we need to meet the challenge. As is evident from the discussion so far this morning, the territory and the areas into which the ICO's work reaches is almost endless. The capabilities that we need we have had to prioritise and focus on the areas of greatest need.

To give you some highlights, or some key examples, our economic analysis and our understanding of the economic impact has been a key strand for us since 2018, since we were given that important duty to have due regard for economic growth in all the work we do. That is an area that we have upskilled, and we continue to do so through our rolling plans. We have also talked today about some of our biggest investigations. Again, that is a new capability that we have needed to develop since 2017-18, that ability to stand up large scale investigations with dozens of investigators to make sure the governance and infrastructure around those is strong and fit for purpose.

There have been a number of challenges on the capacity and capability front. We are very proud of what we have accomplished.

It sounds like a long time ago, 2018, but it is just over two years. In the last 12 months, the pandemic has interrupted that journey, as it has for all organisations. I think we are now in a great place. We have also focused on the culture of the organisation. It is all too easy to focus on the practicalities of capacity and capability, but we were determined not to lose the DNA of the ICO from pre-2017.

We are fundamentally a knowledge-based organisation, meaning we are a people organisation and there are many new members of staff who work for us now compared with 2017, but we have in common the real pride that all our colleagues take in their work and their commitment to the mission and the purpose. Those are key factors for a regulator like us. That is what drives our recruitment and retention, helping us attract the best talent, even though as a public sector body we are clearly not

able to compete with the large private sector, global entities we have talked about today.

Q266 **Mrs Heather Wheeler:** Paul, that is really interesting. Thank you very much for that. It is great that you are so proud of your workforce. That shines out from what you say. You gave me one example. One question people are quite keen to know about is with the eight rights, which have been the most problematic in regulating?

Paul Arnold: I am not sure. The Commissioner may want to come in on this, but I am not sure we would single any out as being particularly problematic. We approached the introduction of GDPR and DPA 18 as just a fundamental upgrade to the UK legislative regime, and it is difficult to single one out. By their very nature they are meant to be complementary and part of a set, so it is really about raising the awareness of organisations of the need for change, making sure we can cut through some of the potential myths or initial reaction to GDPR. It is a fairly complex law.

One thing we are most proud of, and certainly I am, is the work we have done with our SME advice hub, which is us recognising the need to simplify the law for those organisations that need to comply with it but, by definition, their activities are not at the most complex end. We were very keen to avoid small businesses feeling that the new law was a huge burden for them. I think we have made some good strides in packaging up our advice and support through that SME hub, and there are more products coming down the line on that in the next 12 months with the sole intention of simplifying and helping organisations reduce their compliance risk through practical and targeted advice and support.

Q267 **Mrs Heather Wheeler:** I think that is going to be incredibly welcome, because there are many expletives that go in the same sentence as GDPR. There are very few people in the real world doing real jobs who have any interest in GDPR at all. It is a pain in the neck, and you either cannot get information from people because people quote GDPR or you get completely wrapped up in red tape because you have to do GDPR. It is not a blessing in my humble opinion.

This is my last question. The EU still has its elements of data protection. Do you have any insights on how the UK Government will shadow that post-Brexit?

Elizabeth Denham: With the trade and co-operation agreement with the EU, there is a six-month period in which data can continue to flow from the EU to the UK. What is important about that is it gives the EU enough time to come to a decision about whether or not the UK regime is essentially equivalent to that of the EU. That is a technical process. The political process is the legal process, and that is where we are right now.

I think the advantage of the GDPR approach is that other countries around the world are using GDPR as a model to reform their law, so the direction of travel and the trajectory of where the laws are going is to

give people stronger rights. GDPR gets a bad rap from people who say it is just about the paperwork of privacy or having to record all your decisions around data. We are trying to bust that myth because, at its heart, data protection is about respect for customers' and citizens' data and about individuals having the right of agency around their personal data.

It is more important for the reputation of Governments and businesses than it has ever been. We talked a minute ago about millions of users abandoning WhatsApp because they are concerned about data and the terms of service. It is so important that Government, in their policy, take people with them and there is trust and confidence in the digital economy. Stripping down GDPR to its main principles, it is about protection of individuals and certainty for business, and knowing what they are supposed to do to account for data.

Mrs Heather Wheeler: Thank you very much indeed, much appreciated.

Q268 **Damian Hinds:** We talk a lot about "my data" or "people's data". You have used the phrase a lot this morning. In my experience when we talk to our constituents, when people say "my data" they mean things they have disclosed voluntarily for some purpose, like their bank details, their address or their credit card number. When public policy people talk about it, they generally mean something different, which is data about what people do. It is tracking data. Is it possible that, in this debate, we are just talking at totally cross purposes?

Elizabeth Denham: When policymakers are talking about using data better to solve policy problems, to be able to make predictions about what people will do, I agree that is a different matter. I also think people are more concerned about how their data is vacuumed up by especially the private sector to be able to analyse and predict what they will be interested in, for example.

Think about internet advertising. We have an ongoing investigation about the use of personal data to profile individuals and predict and nudge what they may be interested in and what they may do. People are becoming more aware of some of the implications of being tracked, followed, and the data crunched up and used to deliver services to them. We certainly saw that in our credit reporting agency report about the massive amount of data collected about people and how it can be used to deny them credit, for example, or to serve them information, or even not to serve them information, that will change their behaviour. I think people are starting to be more aware and concerned about analytics and algorithms that make decisions about their lives.

Q269 **Damian Hinds:** I want to come on to that, because there is a further level or layer of data that is not really data at all; it is inference. This is using bits of data you have given and bits of data about what you have done to jump to conclusions: because you have these friends, live in this place and like yoga, then you are more likely to be interested in Scottish

independence, the environment or whatever it might be. It is not data in the strict sense at all. It is just stuff people have made up, effectively, by looking at what other people who have similar characteristics do.

Should that be a matter of regulation, the conclusions companies come to and what they do with them in terms of, as you rightly say, how they sell to you, how they credit-score you and also, from the point of view of politicians, the news that is served up to you and the views that are put to you?

Elizabeth Denham: A good example of the debate you are speaking about is on social media companies and whether or not lookalike audiences on a platform like Facebook is personal information. We have come to the conclusion in our investigation that when you have a core of personal information and you are adding potential inferences to it, that can be personal information.

It will be helpful for campaigners and politicians to see our guidance for political campaigning that will help campaigners on the ground—practical, real information on how to use data respectfully in a political campaign and still reach the voters and potential voters in an election, because that has a value too.

Q270 **Damian Hinds:** Yes, but political parties are regulated. They are accountable and, ultimately, they have a brand to protect. There are gazillions of people and machines operating on social media who are not regulated, and the platforms generally are serving up content from them to other individuals rather than from the Labour party or the Conservative party.

Is there a gap in public policy about who is caring about what these algorithms come up with, the inferences they make about people and, therefore, the echo chamber or the bubble they end up being assigned into?

Elizabeth Denham: Is there a gap in content regulation? The Online Harms Bill, the online harms White Paper, go some way to looking at the potential harms people face online, but the ICO also regulates the use of algorithms when they make a significant impact on someone's life.

Ofqual and the use of the algorithm for A-level exams is an example of the use of data and the use of inferences about people that has a real and significant impact on people's lives. We regulate algorithms from that perspective. The gap, I would suggest, is that the ICO can only look at fairness of algorithms when they have a significant effect on someone's life, whether they get a job—

Q271 **Damian Hinds:** I am sorry to interrupt, but I am conscious of time.

It depends on the definition of impact on someone's life and whether the impact on liberal democracy, for example, is indirectly an impact on everybody's life. The effect I am asking about is where people are served up a certain type of content because of their own action and they share it

or whatever, but also because of inferences made about them they will be served up content that goes deeper and deeper, sometimes down a rabbit hole, divides society more, makes people less aware of things they have in common and more aware of things on which they differ. That is injurious, in the first instance, to democracy. I was going to say "arguably," but I do not think it is arguable at all. It is an impact ultimately on all of us. Is anyone caring about that?

Elizabeth Denham: The gap you are talking about is in the societal impacts of the use of algorithmic decision making. We can look at the individual impact, but what effect does the use of tracking and profiling have on society as a whole? Some of those questions are ethical questions, and some of them need a public debate.

Internet advertising is a good example. Who will regulate internet advertising? It can have an effect on people's lives—certain offers are never made, for example, to certain demographic groups in society, so that goes to fairness—but at the end of the day, transparency, fairness, oversight, reputation, all these are of utmost importance on a societal level.

Q272 **Damian Hinds:** Can I turn to the question of children? First, I commend you on the age-appropriate design code. I think it is a fantastic part of your legacy. I remember thinking when it came out, this is amazing. Some of the highlights: in 12, that children profiling should be off by default; and in 8, a platform should collect and take only the minimum amount of personal data they need for the elements of the service the user has actively and knowingly engaged in; in 7, that settings should be high privacy by default; and perhaps the most important of all, either establish age with an appropriate level of certainty or apply these standards to all users. Does it feel to you like that is happening?

Elizabeth Denham: I think the age-appropriate design code is world leading. It is going down a direction of influencing the design of services that are expected to be used by children. It goes to the problem you must hear from your constituents that the internet was not designed for children and the internet needs to take account of children's specific needs. We are proud of the age-appropriate design code. There are jurisdictions around the world, including California, Mexico and Australia, that are looking at the UK's code. The code does not come into force until September 2021.

Q273 **Damian Hinds:** It is in progress now, right?

Elizabeth Denham: Yes.

Q274 **Damian Hinds:** Since September gone. My question is not, is it a great code? I think it is a great code. My question is, is it happening? Do you feel like it is happening?

Elizabeth Denham: I feel we have had impact on the design of services. Last February, before the pandemic struck, my team and I went to Silicon

Valley to socialise the code with the big tech companies. We had meetings with the chief executives across all the big tech companies, and I can tell you that their designers and engineers met with our engineers. There is an ambition for the UK to see this happen to protect UK children, but there is also an interest by the big players. It will come. We are spending the next six months continuing to educate and socialise especially the large platforms on how they can put the code into practice.

It is world-leading work. We consulted extensively with children's groups, technology companies, the gaming industry and civil society to try to get this right. You are right that I am very proud of the work of my office on this, and I want to see how it comes to life in practice. We will be enforcing against the code in September.

Q275 **Damian Hinds:** Thank you. According to the 2019 Ofcom report, a quarter of 10-year-olds who go online claim to have a social media account, and 43% of 11-year-olds. These are claims. This is what they say, of course, and we do not know it for a fact, but these social media platforms typically have a minimum age of 13. Why should we have any faith in the ability of platforms to distinguish between children and adults in this way? This concept of age assurance, as opposed to age verification, how much confidence can we have in that technology?

Elizabeth Denham: The assurance is not the same as requiring a technical identity issue for the companies. Assuring the companies are doing their best to be able to identify individuals who should not be on the platform is important. As identity management and identity management tools progress, we would expect more from companies but, as you know, the state of development of identity management solutions right now is behind the curve, and we have seen that in response to other legislative initiatives. We have to give companies the benefit of the doubt that, when they throw their engineers and designers at a task, they usually have the ability to make it happen. A lot of these big platforms already know a hell of a lot about who the users are, and they can use all kinds of algorithms.

Q276 **Damian Hinds:** To fire adverts at them they certainly do. But there can be a gap between ability and will, I think.

Elizabeth Denham: Hopefully the code gives them the will. We know that if you throw engineers at a problem, if it is to the benefit of the company, they will find a solution. With the code we have incentivised the companies to do a better job of policing who is on their platform at what age.

Q277 **Damian Hinds:** If in a year or two's time a quarter of 10-year-olds and 43% of 11-year-olds responding to the Ofcom survey say they have a social media account and they name the social media platforms they are using, what is the appropriate sanction on those social media companies?

Elizabeth Denham: An investigation and a sanction that is appropriate for the extent of the breach. We have a tool kit full of various sanctions,

and we reserve fines and stop-processing orders for the most serious data breaches.

Q278 **Damian Hinds:** You said a moment ago we should give the benefit of the doubt to companies when they throw their expertise and ability at these things. There is no one who says give the benefit of the doubt to the kids. I wonder, partly because it seems to be very difficult to distinguish between children and adults, which bits of the age-appropriate design do you think would be inappropriate to apply for all users?

Elizabeth Denham: If the company does not follow the identity assurance requirement, none of the provisions of the code, the 15 standards, is out of place for an adult user. I think choice for an adult is really important.

Q279 **Damian Hinds:** You are not suggesting taking away choice, are you, even for the children's code? This is all about defaults and what should be the settings when you come on to the platform. Is there anything in the age-appropriate design code for children that you think should not also apply to the full population?

Elizabeth Denham: I suppose just the first standard, the duty to have regard to the UN convention. Other than that, no. I think a lot of adults would appreciate defaults that are privacy by design—location turned off until an adult decides to turn it on. These are respectful defaults, but the UK Parliament and Government decided that we would focus on children and that is what we have delivered in the code.

Q280 **Damian Hinds:** Can I ask finally about something different: vaccination passports? This Committee has a strong interest in people being able to return to sporting and music events, the travel business, hospitality and so on. In that regard we have talked about various ways of proving having been vaccinated or having had a Covid test. There are also big privacy issues around these questions, and that is also an area this Committee is deeply interested in. As the Minister said at the weekend, we are not a papers-carrying country. What is your take on vaccination passports, on what their usefulness might be and what your concerns would be?

Elizabeth Denham: We would approach a detailed proposal around a vaccination passport or a freedom passport in the way we do with any Government initiative. Is it necessary? Does it work? Does it do what it says on the tin? Is it proportionate? And is there transparency? The question is about necessity because we are talking about personal health information, which is a special category of data that requires control. At the outset we would ask Government the same questions we asked them about the contact tracing app, the same principles.

With immunity passports, some of the issues are beyond data protection. They touch on human rights, on whether or not we will create a two-tier society based on whether you have a jab in the arm. The concern is over whether this is identity by the back door. Those are some of the concerns

I would have, but my approach would be to ask Government, where is the necessity, how will the data be used, is it transparent and is it proportionate to the problem?

For a long time we have carried vaccination certificates on foreign travel to show we have had our typhoid vaccination, for example, and that is a piece of paper. If we start talking about immunity passports that are digital or tacked on to the contact tracing application, those are real questions for policymakers.

Q281 **Alex Davies-Jones:** I would like to go back to explore some of the themes around age and children that you were just discussing with my colleague, Damian Hinds.

As we have heard, most of the social media platforms say users should be 13 or older. WhatsApp is restricted to those who are 16 or more. Are we more hands-off with who should be on social media compared with those who go to the cinema to watch a movie?

Elizabeth Denham: That is such a great question, because the principle behind this is that the laws to protect children online should be the same as the laws to protect children in the analogue world. That is the fundamental principle we are trying to achieve, because why should the internet be a wild west for children? The internet was not designed for children, so how do we solve that problem? We cannot put it in the too-hard pile. We are used to regulations and laws around children buying alcohol or cigarettes, or getting into certain movies. We think the same should apply online. That is the principle behind the age-appropriate design code.

Q282 **Alex Davies-Jones:** I completely agree. On that point, who should set the instruments for social media? Should it be the platforms themselves or the ICO?

Elizabeth Denham: In law the definition of children, in terms of data protection, is those under the age of 13. That is already established in law, but the age-appropriate design code requires companies to deliver content based on the age of the user. A 16-year-old will access information and be able to understand a privacy notice much better than a 13-year-old, and that is why the code is called the age-appropriate design code.

Q283 **Alex Davies-Jones:** You have already stated here today that if a social media platform is shown to have users who are under the age in the age-appropriate code, you would open an investigation. You currently have an ongoing investigation into TikTok. Are you able to tell us more about that investigation and specifically why it is taking so long, longer than originally thought?

Elizabeth Denham: TikTok is a broad investigation, and I cannot speak about a live investigation in public, as I am sure you can appreciate. We are nearing the end of our investigation, and I can tell you what we are

looking at. We are looking at privacy notices and transparency, the sharing of information across borders, the governance and the privacy programme of TikTok. We are looking at messaging systems that are perhaps open to allow adult users to send direct messages to children.

One of the complications with TikTok is that it has recently announced some significant changes to the way it operates, so we have to take that into account in our final report and in any sanction we decide to issue against TikTok. TikTok is changing. There was a potential sale of TikTok, so we had to step back and look at the whole investigation, but we are coming to a conclusion. You will soon see the end of our investigation and action.

Q284 **Alex Davies-Jones:** It would be quite useful for the Committee to have you back once that investigation is completed if possible, so maybe we could follow up on that.

Are some of the issues you just mentioned around the investigation into TikTok and why you are investigating them wider than just TikTok issues?

Elizabeth Denham: Yes. Those same issues are at play with other large platforms. It happens that TikTok is the largest platform used by underage individuals in the UK. It has the greatest number of child users, so it is natural we would look at that. We have had complaints about TikTok. Some of the same issues have been explored by the Federal Trade Commission in the US around, for example, YouTube. These are the same issues about how children's rights are protected.

Q285 **Alex Davies-Jones:** Finally, I would like to ask your opinion on ID cards for 13-year-olds.

Elizabeth Denham: To be used for?

Alex Davies-Jones: It could be used for a range of things, but specifically with regard to age verification on social media.

Elizabeth Denham: Again, I would look at what the purpose is of those identity cards, or identity tokens if they are electronic. Do they work? Are they fit for purpose? What are the privacy implications? I would have to look at a specific contextual example before we could look at transparency, fairness, proportionality and fitness for purpose.

Q286 **Julie Elliott:** Good morning, Elizabeth and Paul. I want to go on to online harms, but just following what Alex and Damian have been talking about, do you think this age 13 thing is working?

Elizabeth Denham: Is your question about whether it is working across all—

Julie Elliott: In general, do you think that young children under 13 are using platforms?

Elizabeth Denham: Yes, I do. I absolutely do.

Q287 **Julie Elliott:** Is there anything we can do about that? I think they are. Do you think there is anything we can do to legislate, probably, or regulate to try to stop people under 13 using these platforms, or do you think it has just gone?

Elizabeth Denham: No, I don't think it has gone. As I say, it is hard, it is difficult, it is challenging. It probably takes a village, including parents working with their children and knowing what their children are accessing online. When it comes to the law and regulation, I think the age-appropriate design code, once it is in force in September, will definitely help. The online harms agenda, which sets out the expectations for conduct and content online, will also be a huge step forward. I think the UK, in its approach to online harms and data protection, is out in front of other jurisdictions in trying to tackle the issue of children online.

Q288 **Julie Elliott:** The Government have given Ofcom the regulation of the online harms area. Do you think that is the right place for it to be? Did you have any discussions with Government Ministers about the possibility of the responsibility for online harms regulation being with your office?

Elizabeth Denham: I am supportive, of course, of the Government's decision, and it is for Government and Parliament to decide who is going to be the online harms leader. Because of Ofcom's experience with broadcasting and content regulation, it is logical for it to take on that responsibility. I am supportive of that.

I think the online harms agenda and the debate around content regulation and moderation will be a noisy one. It will be challenging to balance freedom of speech and security in this space. There is an existing tension between data protection, privacy and content regulation. In order to have content regulation, the regulator and the company are going to have to know more about the users and what is being shared online, so you can see there is a policy tension there.

Q289 **Julie Elliott:** How do you envisage your organisation working with Ofcom on this issue? There must be some sort of overlap, I would have thought.

Elizabeth Denham: If you were going to draw a Venn diagram, you would see the overlap. Essentially, personal information and the kind of profiling that is done about individuals determines the delivery of content. Personal data is used to determine what content is served to a user, so you could see the overlap between Ofcom and the ICO. What has happened is that, in the last 18 months, Ofcom, the ICO and the Competition and Markets Authority have joined together to enact a work programme for the purpose of regulatory coherence. You can see that in digital regulation those areas of competition, content, consumer protection and data protection are coming together like they never have before. The responsibility is also on our shoulders to make sure there is a coherent approach to digital regulation.

Q290 **Julie Elliott:** Do you think the framework puts too much focus on regulating companies, as opposed to minimising harms, or do you think

the balance in the framework is right?

Elizabeth Denham: We have not seen the detail of the framework in a Bill yet, and the ICO, of course, will be interested and will be commentating on legislative proposals. I cannot say without the detail of the framework.

Q291 **Julie Elliott:** Do you have any concerns that heavy regulation might prevent the emergence of competitive platforms to those that currently dominate the landscape in this area?

Elizabeth Denham: That is why competition regulators, content regulators and privacy regulators need to work together to take down some of those walls. I don't think we are worried about defending our perimeters so much as we are interested in making sure that whoever leads an investigation has the public interest in mind.

Julie Elliott: It is very encouraging to hear that you are not working in siloes, because this clearly goes over all sorts of areas. Things will get missed if you work in siloes, so it is very encouraging to hear how you are proposing to work or how you are working. Thank you.

Q292 **Chair:** Elizabeth, you spoke about how algorithms manage content delivery and their importance, and obviously this Committee has heard a lot of evidence recently about how algorithms are dictating swathes of our personal lives. Should algorithms be FOI-able?

Elizabeth Denham: Algorithms that are used by public authorities should be FOI-able to the point where they are explainable, I would say. Obviously, with algorithms, there may be some intellectual property issues as they are provided to public authorities, but what I believe—and this is going back to the transparency agenda—is when public bodies that are subject to FOI use algorithms to affect the population, they should be explainable. People should understand how their data is used. What we have done at the ICO is we have worked with the Alan Turing Institute to produce transparency tools to explain to the public how algorithms work. We have also worked on an algorithm auditing tool, which I think is world leading in terms of the work of the ICO.

Q293 **Chair:** What about private authorities? What about private institutions and their use of algorithms? Should they in some way be FOI-able; maybe not the very technical data but, if you like, the mission statement that lies behind them, the objective of those particular algorithms? Should I not be able to see what the algorithms are going to do in terms of my data and my potential information when I log on to a particular website or use a particular app?

Elizabeth Denham: Under the GDPR and the Data Protection Act 2018, an individual has the right to challenge an algorithmic decision that has effect on their life. In that challenge, there is a transparency requirement to that. The limits of it are, again, that thinking about intellectual property, and you then need a regulator to stand in between the company and the citizen or the consumer. The regulator behind closed

doors can look at the fairness of the data that is used, the training data, and can look at the details of the algorithm and be able to come to a conclusion on whether or not it was fair to use an algorithm that makes a decision. That is where in the private sector it is important to have a regulator in the middle chair.

Q294 **Chair:** An individual having the right to challenge an algorithm and its impact on their daily life, I cannot really imagine that many people, first, knowing what to do and, secondly, getting het up enough to do that. It is quite a narrow field of opportunity, isn't it, in terms of transparency that you have to challenge? Surely it would be better if you had a right of access.

Elizabeth Denham: A right of access involving all the detail of the machine learning that goes into an algorithm, again I think that is why the oversight of algorithmic decision making in both the public sector and the private sector should be moved to a regulator.

Q295 **Chair:** Forgive me, I am not suggesting that someone making an FOI request should receive a huge amount of machine code. We all have lives to live, after all. What I am suggesting is that surely it would be helpful and much more transparent if, for example, I was able to FOI a private company—let us say my life insurer, for instance—and find out exactly what the algorithms it has subjected my information to meant and what the purpose of them was.

Elizabeth Denham: What was the purpose of them? How do they work? How do they make decisions? Are those decisions fair? An individual has those rights but, as you say, it is a narrow field. It takes time and it takes opportunity for an individual to do that. Civil society plays a role here. Individuals do not always know what to complain about, but both the Commissioner's ability to do own-motion investigations and civil society bringing these issues to light are all-important. I think the regulation of algorithms is the most challenging policy area that parliamentarians are going to face in the next three years.

Q296 **Chair:** Surely it would be made easier, though, by a digital bill of rights, for instance. At the moment, what you have said is that individuals have a right to challenge an algorithm and how it impacts their life, but surely it would be easier if we were able to see precisely what the algorithm was meant to do and we had an automatic right of access, a right, a bill of rights.

Elizabeth Denham: I think that GDPR and the Data Protection Act do give the regulator the ability to look behind the curtain and look inside the black box and see what is happening.

Q297 **Chair:** I get that you have the ability to do that, but why don't our constituents have the ability at least to see, to gauge exactly the impact of algorithms on their lives?

Elizabeth Denham: They have the ability to file a subject access request, so that is in law, public and private sector, to find out how their data are used and who it has been shared with. Whether that goes as far as the code, I don't think so, but there is already a right in law through a subject access request that individuals, your constituents, can serve to a company or a public body.

Q298 **Chair:** Yes, a public body, exactly, but not Facebook, for instance.

Elizabeth Denham: Private sector or public sector. That is covered in a subject access request.

Q299 **Chair:** It is subject access but, as I said, it is quite a narrow field. Surely it would be better for individuals, in the same way that they can look to see exactly what their privacy settings are on certain websites or manage cookies, to be able to see precisely what is being applied to them in terms of algorithms.

Elizabeth Denham: I agree that individuals should have the right to see more about how algorithms work, but it is untested how far a subject access request goes with a private sector company. I would be interested to write to you with more detail about the work we are doing in our various auditing tools and transparency tools. If you are interested in that, Chair, I can take some time and write to you.

Chair: Okay, thank you.

Q300 **John Nicolson:** Thank you, Commissioner, for joining us. A criticism I am sure you have heard before is that your office, the ICO, is weak when it comes to enforcement. Could I start off by asking you about the report published on 11 November 2020 into data protection compliance by political parties? You will know what that showed, but for those who have not followed it as closely as some of us, it showed rather disturbing conclusions that the Conservative party had ethnic and religious data on 10 million voters, looking at their country of origin, their ethnic origin and their religion, based on their names. Do you think that is an acceptable thing for the Conservative party to have done?

Elizabeth Denham: No, and in our audit work, where we looked at the practices of all political parties, our recommendation was for any kind of ethnicity data to be deleted. We have evidence that the Conservative party has destroyed or deleted that information. What is really important in the audits that we have done of the political parties is that there is agreement with our audit recommendations for them to comply. Our next report, which is due in June of this year, will outline all the recommendations and how they have or have not been adopted.

Q301 **John Nicolson:** I think the key word there, if I may pick it up, is "recommendation." That is why people sometimes say you are weak on enforcement. It was only a recommendation. You hope the Conservative party has accepted your recommendation, but you did not enforce it. Did you have the legal powers to enforce it? Did you have the legal powers to

require the Conservative party to eliminate all this data that it had assembled in this very inappropriate way?

Elizabeth Denham: The Conservative party's deletion of the data was done in response to our recommendation.

Q302 **John Nicolson:** Could you have ordered it to do so?

Elizabeth Denham: Yes, we could have ordered it to do so in this case—

Q303 **John Nicolson:** Why didn't you?

Elizabeth Denham: We did not have to because it volunteered that it would—

Q304 **John Nicolson:** If it had not volunteered, would you have ordered it to do so?

Elizabeth Denham: Yes, we would. You have seen examples of that in public bodies where we have made a recommendation, it has not been followed and we have ordered the deletion of data. It is engagement first, enforcement second.

Q305 **John Nicolson:** Okay, so you play nice and then you get rough if they do not behave. I think that is probably entirely the right way to treat the Conservative party.

There are three legal bases for data collection. Did the Conservative party's accumulation of this data fall into any of these legal bases? Perhaps you could outline what they are.

Elizabeth Denham: I don't have the audit report in front of me, but I suspect we are looking at the legal bases of consent, legitimate interest or democratic engagement, is that right?

Q306 **John Nicolson:** Yes, I think that is exactly right. You are the expert in this, of course, but that is my understanding of it. You said that the lawful bases under which the parties were processing personal data were not always appropriate. Is there ever a legal basis on which a party could do what the Conservative party did, that is assemble people's names based on their apparent religion?

Elizabeth Denham: Religion and ethnicity are both, like health information, special category data that requires a higher standard for a legal basis to collect. Again, ethnicity is not an acceptable collection of data. There is not a legal basis that allows for the collection of that data.

Q307 **John Nicolson:** So, just to confirm, what the Conservative party did was illegal?

Elizabeth Denham: We made the recommendation that it destroy the data because it did not have the legal basis to collect it.

Q308 **John Nicolson:** That is a roundabout way of saying it is illegal. If there is no legal basis for collecting it, it must be illegal. So, just to confirm, it

was illegal?

Elizabeth Denham: It was illegal to collect the ethnicity data, and that has been destroyed.

Q309 **John Nicolson:** I am glad you have been able to confirm that because John Whittingdale, the Minister, has repeatedly said in the House of Commons that what it did was legal. You put it firmly on the record that what the Conservative party did was illegal and, therefore, what Mr Whittingdale keeps asserting is simply untrue?

Elizabeth Denham: I think Mr Whittingdale suggested that you ask me in my appearance about specific collection of data. Again, we are talking about the collection of ethnicity data. The Conservative party and all the other parties had a series of recommendations from our office, which we are following up to make sure they comply.

Q310 **John Nicolson:** People like clear answers in this. You have confirmed that it was not legal to do what the Conservative party did; therefore, it was illegal. When Mr Whittingdale says on the Floor of the House of Commons that what the Conservative party did was legal, he is simply wrong. That is a yes or no answer. He is allowed to be wrong. Goodness knows, politicians are allowed to be wrong about things. There is an absolutely logical conclusion to what you have said to me, and I think it just requires a simple confirmation: Mr Whittingdale is wrong.

Elizabeth Denham: I told you what our report said about the collection of ethnicity data. Again, I do not have what Mr Whittingdale said before—

Q311 **John Nicolson:** I can tell you, because I asked him the question. He said that what the party had done was not illegal, and you have just confirmed it was illegal, so he was wrong.

Elizabeth Denham: It was illegal to collect ethnicity—

Q312 **John Nicolson:** Yes, so he was wrong.

Elizabeth Denham: That is what our report says.

Q313 **John Nicolson:** Commissioner, you should be a politician. There is nothing wrong with saying the word "yes," but let's move on because I feel I am flogging this to death when your answers are pretty obvious.

You mentioned other political parties, and again Mr Whittingdale and others have tried to suggest that all parties were equally bad on this. It is worth noting, is it not, that according to your report the SNP, Plaid Cymru and the DUP, all represented in Parliament, did not do this? It is not true that all parties did the same thing.

Elizabeth Denham: The recommendations in our report were on many other aspects of practice, not just the collection of ethnicity data. There were many things that needed improvement across all the political parties. You have to look at the extent of the report and all of the issues we examined, not just whether or not ethnicity data was collected.

Q314 **John Nicolson:** I accept that, and you made recommendations across the board. I am not just singling out my own party; the SNP, the DUP and Plaid Cymru did not do what the Conservative party did. Again, Mr Whittingdale implied that they did. That is wrong, and I hope you are able to confirm that. They did not accumulate data based on ethnicity and religion.

Elizabeth Denham: I can speak for the ethnicity piece. I would have to go back and look at the audits for religion, but I agree that the other parties were not collecting ethnicity data. However—

Q315 **John Nicolson:** That is my understanding. That is the question I wanted to confirm.

Can I turn very quickly—and I am sure some of my other colleagues want to come in on this—to the question of track and trace? With track and trace, were you concerned about the potential for mass data breaches?

Elizabeth Denham: The test and trace programme is something that we have been actively advising along the way. As you know, the test and trace programme was set up at pace to be able to deal with a pandemic, the public health emergency. Our approach is the same as we always do, to be agile and get in there and give advice and improve practice on the ground. Test and trace is a system that we will be auditing, and the test and trace programme knows and is aware that we are starting to audit how it uses data and whether or not it has been discarded.

Q316 **John Nicolson:** Were you worried about the private company that was involved in this? It did not exactly have the most glorious track record, did it?

Elizabeth Denham: Our audit is looking at the security of data, the governance of data, the collection of data and the disposal of the data at the end of the day. We are doing a wholesale audit on the data.

Q317 **John Nicolson:** Finally, were you concerned about the plans to give the track and trace data to the police?

Elizabeth Denham: My understanding is that the data was not given to the police. That was a consideration, but I would have to—

Q318 **John Nicolson:** Would you have been concerned had it been given to the police?

Elizabeth Denham: Yes, because I believe the test and trace programme was set up to deal with a public health emergency, and it was not necessary to share that information with law enforcement.

John Nicolson: Thank you very much.

Q319 **Giles Watling:** In our evidence session back in September, Theo Bertram of TikTok said that UK user data was held in Singapore and the US but that it is moving all that to Ireland. Did you know that it is still keeping the data on servers in the US and Singapore?

Elizabeth Denham: I am not aware of where the data is held. I am sure that my team that is doing the investigation is aware of that. What is important in terms of where the data is held is that UK legislation has extraterritoriality. We have the ability to investigate wherever the data is held.

Q320 **Giles Watling:** Theo Bertram said that the EU does not recognise the US as a safe place for this storage. Would you agree with that?

Elizabeth Denham: The challenge right now is that the privacy shield, which was the bridge between Europe and the US that allowed data to flow with protection, was struck down by the courts. Now there is work going on between the EU and the US to find another mechanism for the safe transfer of data. It is not that the data is unsafe, it is looking at what kind of oversight and protection there is of European data in the US and Singapore.

Q321 **Giles Watling:** Do you have enough access to that information at the ICO?

Elizabeth Denham: We have worked to gain access to data held in the US in various investigations, including Equifax. We have the ability to work with other regulators to be able to carry out our enforcement activities. What is really strong about the ICO is that I am the chair of the Global Privacy Assembly and my deputy is the chair of the OECD privacy committee. That brings us into positive and good relationships to collaborate with regulators around the world, which we do. I think that helps to safeguard UK citizens' interests.

Q322 **Giles Watling:** Can you say with absolute security that you are satisfied with the access you have to US data?

Elizabeth Denham: I am satisfied now. Again, carrying out enforcement activities and investigations in other countries requires us to have a relationship, a memorandum of understanding, with regulators that are on the ground there.

Q323 **Giles Watling:** Thank you for that. Moving back to TikTok, it says it is moving all its data to Ireland. Do you have any evidence to show that it has done that or is complying with that?

Elizabeth Denham: Again, I can write to you about what our team has found, but I do not have that knowledge at my fingertips right now.

Q324 **Giles Watling:** That would be good. Do you think it is sufficient for a company such as TikTok merely to have an ambition to comply with the regulations, or do you think it should absolutely comply with the regulations?

Elizabeth Denham: No, it should absolutely comply with the regulations and that is why we are doing a deep dive investigation into TikTok.

Q325 **Giles Watling:** That is very good. I was pleased, by the way, when you

said earlier that you are slightly reticent about the idea of ID cards. I think civil liberties must be defended at all times, so thank you for that.

Moving on, you were talking earlier about the ePrivacy Regulation. Do you think we should be ready to enact legislation equivalent to that here?

Elizabeth Denham: You are talking specifically about the Privacy and Electronic—

Giles Watling: Yes, the beefed-up ePrivacy Directive, which is now the ePrivacy Regulation. Should we copy the EU on this?

Elizabeth Denham: What we hear about most in terms of public concern is nuisance marketing, the scams and the criminal activity that go on with the use of personal information in electronic marketing. The public care most about two things. They care about nuisance calls and nuisance texts, and especially vulnerable populations falling prey to that. Secondly, they care about the security of their data, data breaches and the amount of data that is for sale on the dark web. Those are the two highest level of concerns for UK citizens.

I think we need electronic communication regulation, absolutely, but I think that the cookie regulation and the way cookies work on the internet is not meaningful control and regulation. I do think that people are tired of cookie notices. They click "accept", "accept", and whether or not that is actually meaningful control for individuals is an open question for policymakers.

Q326 **Giles Watling:** I am guilty of that as well, because you want to get on with it when you go to a site. It says "cookie" and you just accept it, so it is meaningless. Going back to Cambridge Analytica, all this data collection and all this stuff that irritates people all the time, this micro-targeting of advertising information and so forth, are we getting on top of it finally? It has been going on for years now.

Elizabeth Denham: I think we are. The public does not understand how internet advertising works. We read about it in the press, we read specialist reports, but I think the UK is getting on top of this. The Digital Markets Unit, the work that the Competition and Markets Authority is doing on investigating internet advertising, the work that we are doing to investigate real-time bidding that affects individuals, I do think that regulators are getting on top of that. What needs to be clear is who is ultimately responsible for overseeing internet advertising. That is an important question.

Q327 **Giles Watling:** Who do you think that should be?

Elizabeth Denham: From a competition aspect, it is the CMA; and from the use of personal data and the use of personal data to micro-target, that is our office. There are also other bodies involved in looking at fairness in advertising.

Q328 **Giles Watling:** Thank you. That is very clear. We have moved into a

brave new world with Brexit and so forth, but if we have this data protection regime with GDPR and we do not have the ePrivacy Regulation that the EU has, would that undermine our ability to ensure robust data protection in the future?

Elizabeth Denham: It could do. I think the electronic marketing regulation and the GDPR need to work more closely together and to reflect the same standards around consent, for example. That is really important.

Giles Watling: Good, thank you for saying that. Thank you very much.

Q329 **Chair:** To pick up on a couple of points that you mentioned in your answers to Giles, in relation to the CMA and its work, do you think competition law is a means by which to make large social media companies behave as better citizens?

Elizabeth Denham: I think it is going to take a village to change the behaviour of companies of a size we have never seen before. It is a combination of the accountability and governance that we expect through competition law, content regulation and data protection. I think those siloes and those walls are coming down, and we have an opportunity to choreograph our response to big tech using the expertise at all three of those regulators. What we need is a coherent and co-ordinated response to social media and technology companies.

Q330 **Chair:** To clarify that, you say it will take a village. I have never heard that before. I come from a village, so maybe that is why. Does that basically mean lots of different organisations?

Elizabeth Denham: No, when I say it takes a village, it is really important that we get the right law in place, so that is policymakers and parliamentarians. It is going to take the public to deeply care and be prepared to change providers, for example, if they are unhappy. It is going to take the regulators to be bold and to do the work that they need to do. That is what I mean by a village. It takes civil society, it takes individuals to vote with their feet, and it takes the regulators to have the right approach.

Q331 **Chair:** Thank you for clarifying that. We also very briefly touched on ID cards, at least Giles did. I am very much in agreement with him; I cannot think of anything worse. Do you think that management of the pandemic would have been easier with ID cards or some form of ID token, as you mentioned before?

Elizabeth Denham: It could have been, but none of us saw what we had to deal with. None of us saw it coming in 2020. What has happened in the pandemic is a huge acceleration in the use of data, a huge acceleration in the take-up of digital services to be able to run our lives in isolation, and what has happened is we have fast-tracked. We have fast-tracked what would have taken us five years. Now what you have sitting in your lap as policymakers is how you go forward to grapple with identity

management, ID cards, and employees working from home and the rules and regulations around that.

ID cards need very careful consideration. Again, I can see that vaccine passports of some sort would be useful. I can see that, but people have to trust the Government when they bring in these initiatives to understand what the purpose is, to narrow it as much as possible, and to make sure at the end of the day that their civil liberties, human rights and data protection are respected.

Q332 **Clive Efford:** Elizabeth, you updated your guidance to employers back in 2018. When do you expect to update it again, and how often do you think you will do that updating in the future?

Elizabeth Denham: An update to the 2018 guidance is imminent, because during the pandemic we have been giving a lot of advice to employees and employers about the collection of health data in the workplace and about the need or the desire to surveil employees to make sure they are effectively working from home. Again, I talked about the acceleration of the use of digital tools in the pandemic. In the employment field, it has accelerated extremely quickly. We have been giving just-in-time advice to unions, employees and employers, and we will create a hub of guidance and an update of our guidance because it is absolutely needed in this environment.

Q333 **Clive Efford:** What practices have you uncovered that are taking place? Some trade unions, I understand, have written to you expressing concern about the lengths that some employers are going to to monitor what staff are doing, and that may be infringing on their personal privacy. Is there anything that has alarmed you?

Elizabeth Denham: An increase in digital keystroke monitoring and other types of monitoring of how long somebody is on their computer, how long it takes them to answer a call, that kind of surveillance. Going back to the principles in law, it has to be necessary, it has to be transparent, it has to be fair, and an individual has a right to see what their employer is collecting on them. All those principles apply but, just like everything else in the pandemic, employers are no different and they are trying to protect their workplace and their assets. Part of that is more intensive surveillance of their employees, but all those practices have to follow the principles in the law.

Q334 **Clive Efford:** Have you discovered any infringements in terms of inappropriate use of personal data relating to employees?

Elizabeth Denham: I haven't seen that directly, but the question about how much of an employee's health information an employer has a right to is a significant issue. "No jab, no job" and those kinds of issues are real issues that we have to grapple with, not just in data protection but in employment legislation and human rights as well.

Q335 **Clive Efford:** Even before Covid, we saw that technology was being used

in places like large warehousing, where pickers operate, to monitor what staff are doing. It is very intimidatory for people who are in a very weak position, often in very low-paid work without trade union representation. Are you concerned that Covid has created an environment where that sort of repressive regime can be imposed more easily?

Elizabeth Denham: That is why civil society, employee groups and oversight bodies like ours have to pay attention to what is happening in the pandemic and in the economic recovery period as well. It is not just this current period, as we know we will go through years of economic recovery where new uses of data will be proposed and, again, those same principles need to apply.

Q336 **Clive Efford:** I want to move on to the data breach at BA in 2018. Do you think that BA responded appropriately and adequately to that breach?

Elizabeth Denham: It did. The tragedy and the disappointment is that BA did not take good care of customer data. There were large gaps in the security of data and, therefore, the breach. The fines that we issued both to the Marriott and to BA were reduced partly because of pandemic pragmatism and the hit that the pandemic has had on the hospitality industry.

Q337 **Clive Efford:** Can I come to that issue about the level of the fine? You say that you took into consideration the impact of the pandemic on those companies. Does that mean that, if similar breaches were to occur outside of the pandemic, people can expect bigger fines?

Elizabeth Denham: Yes. Again, the reason that the fines were lowered in that case was partly because of the additional information that we received in submission from British Airways and the Marriott hotel, but also because of the economic circumstances those organisations were facing. A £20 million fine is still a significant fine compared with the cap of £500,000 that we had under the previous legislation.

Q338 **Clive Efford:** BA was fined £183 million. What was the worst aspect of it that made you impose that size of fine?

Elizabeth Denham: That was a recommended fine. The actual fine was £20 million.

Q339 **Clive Efford:** But what made you recommend that level?

Elizabeth Denham: The number of individual clients who were affected and the detail of the information that had been breached, including passports and so on. It was a significant issue because of the number of people affected, the detail and the sensitivity of the information that was breached, and also the fact that it was entirely preventable.

Q340 **Clive Efford:** Do you think that the fines are effective? Do you think they make companies sit up and respect customers' data more?

Elizabeth Denham: I think that the level of fines and sanctions in GDPR are important because they get the attention of the boardroom. Since GDPR has been passed, there has been more investment in data security than at any time in the past. Part of that is probably fear of sanctions and fear of fines. Let me say that GDPR is not all about fines. The law is only two and a half years old, so there is still a journey with this law. One of the most significant concerns of the UK public is data security, and that is why the fines are an important deterrent. They are not the only tool in the toolbox that we use, though.

Q341 **Clive Efford:** Do you think the Government do enough to protect people's data, particularly data relating to their identity?

Elizabeth Denham: I think the Government still have a way to go to protect systems, especially legacy systems, but the general trajectory is better sensitivity, more control and more security to protect data. That is also the way to ensure public trust in the future.

Q342 **Clive Efford:** Should that be a duty of the Government?

Elizabeth Denham: It is a duty of the Government to have reasonable safeguards in place to protect personal data. That is part of the law.

Q343 **Clive Efford:** Are there sufficient safeguards in place for people who suffer identity theft to prove who they are and get their identity back?

Elizabeth Denham: That is a whole area of deep public concern as well. We do not have a role in compensating individuals who are harmed by identity theft. The financial ombudsman and the FCA are in that space.

Q344 **Clive Efford:** Do you have any suggestions for steps that the Government should take in order to protect people from identity theft? After all, it is their data that starts the process.

Elizabeth Denham: The National Cyber Security Centre has a lot of advice for individuals and organisations. It has done a really good job in its security essentials programme to help Government and local government, small government, to comply with reasonable safeguards and standards to protect data.

Q345 **Clive Efford:** Last question: do you think that companies—train companies when they sell tickets, for instance—ask for data that is not necessarily germane to the transaction, that too much unnecessary data is being sought at times?

Elizabeth Denham: We have seen many complaints about overcollection of information. Collecting too much information and storing too much information is a significant risk for companies. Again, you have more data that could be exposed and could be used. If there is a data breach, retaining unnecessary data is just going to exacerbate the problem that the company has found. We have seen that in many of our data breaches, data that should not have been collected or data that should

not have been retained exposed the company to claims and sanctions by regulators.

Q346 **Damian Green:** Commissioner, we are in the middle of holding an investigation into the music industry, streaming and payments to artists and so on. The use of data has become an interesting subset of that. Many of the stakeholders we have had in front of us have asked for the standardisation of data when it comes to music rights so that everyone gets paid properly and nobody is missed out. Within the current UK regulatory framework, who should this fall to? Is it you or is it someone else, or isn't there any kind of regulatory framework for that?

Elizabeth Denham: For me to understand, is this really about copyright?

Damian Green: No, not really. It is about the use of the data, which drives a lot of consumption of music on streaming services. Boiling it down, the artists and songwriters are complaining to us that this is kept privately between the streaming services and the big record labels. They cannot tell whether they are being paid fairly or not. It is that use of data and the keeping of that data private that might impinge on your realm of powers. I just wondered if it does, or if this is the first time anyone has asked you this type of question.

Elizabeth Denham: This is the first time I have been asked the question. I wonder if I could take it away and write to you in response. Again, we are in the business of regulating collection, use and disclosure of personal information. If we are talking about, I guess, the number of hits on a certain song, that might be information that determines how the musician is paid. That is the platform and the songwriter, but the personal information is the area that we are in. Paul, if you are listening, can you help us out here?

Paul Arnold: I am certainly listening, but I think we will need to take that away and look into it. It is not something that I have come across or been asked either, I am afraid.

Q347 **Damian Green:** Expanding it a bit then, it sounds to you at first instance as though this is a commercial arrangement between two bodies and, therefore, would not fall under any definition of personal data that you deal with?

Elizabeth Denham: I think so. As Paul said, I have not come across this but it sounds like a commercial relationship involving non-personal data.

Q348 **Damian Green:** I suppose that leads on to the question of whether there are any mechanisms for regulating this type of non-personal data. You will know as well as anyone, obviously, what the boundaries of your powers are, but does it feel like this is just a gap, that there just is not any regulation of this type of thing and that if the Committee or anyone else came to the conclusion that perhaps there ought to be some kind of regulation, not least on transparency in the use of algorithms in this type of activity, we would have to start from scratch with primary legislation?

Elizabeth Denham: I am not sure. I would like to take that away. If algorithms are used but the data is non-personal, then it is definitely not us. Let me have a think on that one and we will write to you.

Damian Green: Okay, that is fair enough.

Q349 **Chair:** I thought that was a really pertinent question, and it feeds into the questions I was asking earlier in the session about whether an individual has the right to challenge an algorithm that impacts their life, whether it is a private or a public company. To a certain extent, a cartel, effectively, with non-transparent algorithms is managing a market. That then means the producers, the artists if you like, within the music industry are not gaining fair recompense for their work. Is that not a public harm?

Elizabeth Denham: It could be, but is that not a contractual issue?

Q350 **Chair:** If the means by which this cartel—and I am not judging it, I am just using that phrase for ease—is arranging its business approach is by means of algorithms, and that is not clearly in a contract, the power balance is enormously in its favour and there is no power. The power of an individual to have a right of challenge to an algorithm does not have any bearing on that, does it?

Elizabeth Denham: Again, that is a complicated issue. I would like to have a further discussion with you about that because, when I think about transparency and algorithms, I am thinking of individuals being able to challenge that.

Q351 **Chair:** Okay, we will pick this up in writing if we can, because I think it is a really important area and it moves into our other inquiry.

Finally, we are going back to where we were at the start when Kevin talked about Cambridge Analytica. I remember interviewing you at that particular time on quite a few occasions. I think you were in every quarter. Looking back on it now, what is your feeling? What reflections do you have in terms of that period, of the circus that went around Cambridge Analytica and the fact that there was a degree of using it as a means by which to undermine the referendum result?

Elizabeth Denham: We were very careful. Because we are a non-partisan, apolitical, evidence-based regulator, it was challenging for us to do our work. It felt like the investigation was on the telly every night and witnesses were popping up here, there and everywhere. Carrying out a serious investigation in the public domain like that was extraordinary.

We had to take comments from witnesses. We had many witnesses who refused to be interviewed by us but were happy to talk on the 6 o'clock news. That makes it really difficult, and I do not have the ability to compel individuals to be interviewed. I do not have that power in law. Again, there would be lots of claims for which we had to interview those who were willing to be interviewed. We had to look at the evidence and we had to be able to keep Government and Parliament up to date. As you

said, I was in four times one year when we were investigating. Part of our investigation was behind closed doors, and the rest of it seemed to be conducted in the public domain. It was very challenging, but at the end of the day—

Q352 **Chair:** Sorry to cut across you. Did any of that force your hand or change the way in which you approached things? My perception was that there was a degree of confirmation bias about much of the reporting around this. We had much lauded, prize-winning journalists coming out with quite bizarre conspiracy theories, diagrams and that sort of thing. We had, frankly, disjointed Netflix films. We had witnesses who claimed to be whistleblowers but were actually in the market for selling information in the same way as Cambridge Analytica was being accused of. Is your feeling that perhaps there was a circus, there was confirmation bias and that effectively you were being used as a means by which to bring about a political objective, as in the undermining of a democratic decision of the people of this country?

Elizabeth Denham: That is not what we were investigating. That may be coloured by others, but the reason we investigated the use of data in political campaigns, and we had started that investigation before the news about Cambridge Analytica and Facebook broke—because we started that investigation months before *Channel 4 News* ran their programme—was because we could see the train leaving the station in terms of the technology developments and the behavioural advertising models that were being used in democratic elections before there had been any kind of public debate. The question that was driving me forward was: is it acceptable that behavioural advertising techniques that we are used to selling us holidays and trainers are transposed into the democratic realm? Those were the questions that we were trying to answer, and we tried our best to use the evidence we had in front of us.

Gosh, it makes a good narrative, you have a lot of characters involved in that story, but what was really important is that we were able to look at the data, to interview those who were willing to talk to us, and we produced objective reports. We have not finished that work because, again, it led to investigations of credit reporting agencies and data brokers. What we did was we looked at the whole ecosystem of political campaigning, and we will get to a good place if we have started a debate that needs to be had.

Q353 **Chair:** Who was not willing to speak to you? You said that they were happy to appear on the 6 o'clock news or the front page of *The Guardian*. Brittany Kaiser, the star of the Netflix programme, was not willing to speak to you at all, was she?

Elizabeth Denham: No.

Q354 **Chair:** No, okay. Any of the so-called whistleblowers, Wylie et al?

Elizabeth Denham: I don't want to give you any inaccurate information, so I would feel better if I could write to you.

Chair: Yes, okay, that would be interesting. Because you have referenced it in the public session, I would release that particular information if it comes along, as you mentioned it as individuals. Just for posterity's sake, we need to know that people who were claiming to be whistleblowers did not wish to speak to you, a regulator with an important role in this. I think that is quite important information.

Anyway, thank you very much for your openness today and your willingness to field questions on a massive variety of issues. It has been much appreciated. Elizabeth and Paul, thank you very much. That concludes our session.