



HOUSE OF LORDS

Select Committee on Communications

Corrected oral evidence:
The internet: to regulate or not to regulate

Tuesday 11 September 2018

3.30 pm

[Watch the meeting](#)

Members present: Lord Gilbert of Panteg (Chairman); Lord Allen of Kensington; Baroness Benjamin; Baroness Bertin; Baroness Bonham-Carter of Yarnbury; The Bishop of Chelmsford; Lord Goodlad; Lord Gordon of Strathblane.

Evidence Session No. 13

Heard in Public

Questions 113-121

Witness

I: Elizabeth Denham, Information Commissioner, Information Commissioner's Office (ICO).

USE OF THE TRANSCRIPT

This is a corrected transcript of evidence taken in public and webcast on www.parliamentlive.tv.

Examination of witness

Elizabeth Denham.

Q113 **The Chairman:** I am very happy to welcome Elizabeth Denham, the Information Commissioner, to this evidence session of our inquiry into regulation of the internet. Commissioner, thank you for your time and for being with us this afternoon. I will ask you to say a few words of introduction in a moment. I remind members of the Committee to declare any relevant interests at an appropriate point. I would like to make a declaration myself. I worked for the group Britain Stronger in Europe during the campaign to remain in the EU before the 2016 referendum and I was consultant to the Conservative Party at the last general election campaign. Both these organisations have been of interest to the Commissioner with respect to the use of personal data during those campaigns. The activities have not been the subject of this Committee's inquiry and I do not anticipate that they will be at issue today. I have not personally been the subject of any requests from the Commissioner and I no longer have any role with either Britain Stronger in Europe or for the Conservative Party other than party membership. I make this declaration for the sake of full disclosure.

Commissioner, thank you again for your time. I hope you have been following our inquiry, which is broad in nature, into the future regulation of the internet. One of the areas that we are particularly interested in is how to have a horizon-scanning approach so that we are not just reacting to issues that cause public concern but have a public policy-making approach that is abreast of issues as they develop, as technology develops and work in the area becomes of public interest. We would like to discuss that with you at some point. Today's session will be recorded and a transcript will be taken.

Commissioner, can you start by describing the current role of your office—its role in the online regulatory framework—and tell us a little bit about your resources, the challenges of doing your work within those resources and whether they are sufficient for the role that you undertake?

Elizabeth Denham: Thank you very much for the invitation to be here to discuss these issues with you. It is an interesting inquiry. As the UK's regulator for data protection, my office has a crucial role in the regulation of activities on the internet as they relate to personal data. As we know, personal data underpins so much of the commercial activities that are happening online. We definitely have a horizontal role across all industries.

The ICO regulates 11 pieces of legislation and includes the general data protection regulation, the Data Protection Act 2018 and the Freedom of Information Act as well. We are already a regulator that is well versed in balancing openness generally, certainly on the internet, with the private space in the public interest. We are very much engaged in these activities. Many of the activities—the elements of the internet—are regulated. You have heard that from many of the witnesses who have

appeared before you. We do not think that it is the Wild West. It is regulated, and personal data that underpins so much of the digital economy has just been given a once-in-a-generation reboot regarding the powers of the regulator, the increase in our jurisdictional reach, sanctions against companies that break the law but also new rights for consumers and citizens.

Whether you are talking about the greengrocer or Google, these activities involve citizens' data online or offline and they are already regulated. One way of thinking about it is that data protection is medium-blind. From online harms, which you have been discussing, to legal and illegal content, fake news to data monopolies, data interoperability and the responsibilities of the tech giants, these are broad and complex issues and data protection is a thread that runs throughout.

One thing that is clear to me and which is clear to many commentators in the public is that things cannot continue the way that they are. The time has come to have more rules and more controls for individuals to protect against some of the harms that are of deep public concern.

When it comes to data protection law, maybe in comparison to other areas of regulation our law in the UK is world leading and, because it has just had a reboot, it is fit for purpose for the digital age. When we are undertaking reviews of regulating activities on the internet, it is right that we look deeply at the types of harms, identify them clearly, look at the existing levels of regulation and the reach of regulators, look at the gaps and then, only after that analysis, decide whether there needs to be a new regulator or new regulations. This kind of deep inquiry and consultation is really important.

You wanted to ask me whether I had the resources to do the job. If you had asked me that question a year ago I would have had a different answer. I think the law is fit for purpose for the digital age. The Government have given me, effective from January, a pay flexibility that allows me to better recruit experts, especially technical experts and legal experts to help me with my work, and the Government have also provided a new fee regime for the ICO. Our budget has gone up 58% since last year and that allows us to do some of the work that we really need to do. A year ago, however, I would have had a different answer.

The Chairman: Could I ask you a little bit more about that? You have the resources to attract the kind of expertise you need. Presumably you are competing with tech businesses in many cases to attract recruits. Is there a skills shortage and are there sufficient people out there, regardless of whether or not you have the resources to fund them?

Elizabeth Denham: It is helpful that we have pay flexibility and we have the resources to be able to attract them but there is a skills shortage out there. What we have to offer is perhaps different from what tech companies have to offer. We are doing socially relevant work. We have secondment programmes that bring people in from the private sector and the technology sector. We have an academic fellowship where we have

just attracted an expert on AI to help us with setting up our programme for auditing algorithms. We are trying to reach into the private sector and trying to do what we can, but I agree that there is a skills shortage in this area. If you look at one of the hot jobs now in the jobs pages, it is data protection officer. It used to be a back-room area of practice but is definitely a front-burner now. We are competing therefore with large companies and technologists.

The Chairman: You said, as indeed did many of our witnesses from across the industry, that we have world-leading regulation in this country and that that applies to your organisation and fellow regulators. That is world-leading with regard to the quality of the regulation itself, but what role do you play with international regulators? How do you demonstrate that global leadership?

Elizabeth Denham: With our European counterparts and colleagues, we are part of the European Data Protection Board and we have led in 40% of all the guidelines that have been written to interpret the GDPR. We are collaborating on enforcement and policy work not just with our European colleagues but with international players. The ICO is a member of the Common Thread Network, which is a connection of Commonwealth countries. We are a participant and leader in the Global Privacy Enforcement Network, which has over 50 regulators around the world. We work with the Federal Trade Commission under the terms of a memorandum of understanding. We are globally connected and that work needs to continue after exiting the European Union. It will be very important that the ICO continues to play a role. We are the largest data protection regulator in the world in terms of resources and numbers. We are now leading an investigation that has the interests of all the players in the world into political campaigns and the use of data analytics. The world is watching this investigation.

The Chairman: Thank you. We may well come back to the international dimension. Baroness Bonham-Carter.

Baroness Bonham-Carter of Yarnbury: May I pick up on the enforcement point? We are talking about big companies. Do some respond to fines or whatever by just shrugging their shoulders and putting it down to a business expense?

Elizabeth Denham: In the previous regime, when our fining power was a maximum of £500,000, that might have been true, but with our new fining powers of up to 4% of global turnover it is much more significant. In fact, with the big global companies it is not even the fine that will have them concerned but the hit to the reputation and the loss in users' trust of platforms if a regulator imposes a fine for contravention of the law. You will know that we have issued our notice of intent against Facebook for the maximum fine under the old regime and we will be settling that issue fairly soon.

Q114 **Lord Gordon of Strathblane:** Various witnesses in written evidence have pointed to the number of different organisations in Britain regulating

the internet to some degree or another and said that this could be confusing. What is the best way of handling this? Could we have a co-ordinating body that makes sure that they are all singing from the same hymn sheet on principles at least, or do we need a meta-regulator standing above all of them?

Elizabeth Denham: Ultimately, it is for Parliament and policymakers to decide how many regulators there should be and what they are responsible for. Let me tell you what we do right now. Because the ICO has a horizontal reach across all the activities on the internet, we work with industry regulators very closely. We are working with the FCA, for example, on a very similar sandbox initiative so that we are looking at fintech projects that the FCA is looking at in some of the same ways. We have seconded someone from the FCA to help us build our sandbox. We are working with Ofcom. In a week or so we will be releasing research that we have co-operated and collaborated on. We have worked with the Electoral Commission on some of the policy recommendations. It is not ad hoc.

Lord Gordon of Strathblane: And with regard to standards, presumably you liaise with them. Do you think it needs a separate body or can it be done by harmonised co-operation?

Elizabeth Denham: We have harmonised co-operation, but it is probably not well known how much work is done under the covers. There would be a role for a co-ordinating body that is forward looking—not reactive but proactive and identifying future gaps in the law and assisting the regulators in getting the resources that they need. Maybe there are law changes that need to happen because this is not a static area. It is moving very quickly.

I like the idea of a co-ordinating body. There is a new body in town called the Center for Data Innovation and maybe there is a fit for a body like that to draw things together. The last comment I will make is that the economic regulators are getting together to look at whether or not there is a harmonised or consistent way that we can look at algorithmic bias and algorithmic transparency. There is a lot of work to do.

Q115 **Lord Goodlad:** I want to ask about data protection law being described as principles-based, being based as it is on the data protection principles. In your view, what are the advantages and disadvantages of using principles-based regulation?

Elizabeth Denham: Principles-based regulation works for an area of law that is fast changing and fast moving. The principles-based legislation, which data protection law is, allows for more detail to be developed through guidelines, codes of practice and certification that flow from the principles. Some commercial entities like more prescriptive or rules-based legislation because there is certainty, but it is not very flexible; it is rigid and it is not future-focused. One example is that in data protection law there is only one principle about data security. It says that organisations have to have appropriate safeguards in place to protect against misuse

and unauthorised access. The question we always get is: what is appropriate? From there it is context that you have to look at. How sensitive is the data? What are the threats and risks on the horizon? If the law said that everybody had to have 256-bit encryption, that would be outdated. What is appropriate, therefore, is going to change depending on the environment. That said, we get many complaints from companies that say, "Just tell us what 'good' looks like. Just tell us what we are supposed to do". The beauty of the GDPR is that it provides for codes of conduct and certification and co-regulation in specific areas of practice.

The Chairman: To follow through on the principles-based regulation, you talked about how we need to be forward looking, which means applying those principles to risks as they develop and presumably applying solutions as new solutions become available. Who in this mix is responsible for that broad, forward-looking approach for scanning the horizon, identifying future risks, future technological developments, changes in behaviour in tech companies, different remediations and what might be happening around the world? This is not just about data; it is about a whole range of regulatory approaches. Who in the mix is responsible for that?

Elizabeth Denham: There is not one regulator or one authority that is looking that far to the horizon. We are doing that work in data protection but are not necessarily looking at changes in consumer attitudes or behavioural changes or new societal risks or ethical considerations. That is not the job of the data protection regulator. You talked about a co-ordinating body—a body that is looking to the future. That is maybe a solution that we need to look for in the UK.

The Chairman: You do not seem to be formally advocating such a body, but is it a possible solution that might work across regulators?

Elizabeth Denham: It could do and you would have to have a lot of different types of expertise on a body like that. Societal attitudes change. I sense a change in consumer concern over hacks on the internet, over data protection issues, over profiling and targeting in a way that was not there three years ago. Watching for these societal concerns and changes, while it is for Parliament, there could also be an expert body.

Q116 **Baroness Bertin:** I would like to declare an interest. I work for BT. I want to bring you back to some of your comments in your introduction about harm from the internet and particularly to talk about ethical design and what principles you think should underpin ethical design.

Elizabeth Denham: From where I sit, I am hearing that people are more and more concerned about both illegal content on the internet and legal content where it does not quite reach the threshold of a criminal act. There is concern about that. One of the designs that we need for the internet is protection against illegal content and offensive content, especially when it comes to children and vulnerable adults. Any kind of internet design needs to take that into account.

Baroness Bertin: Some of our witnesses have said that in truth designers are not going to ethically design unless they are forced to. Would you agree with that analysis?

Elizabeth Denham: I think that is right. One of the interesting tasks that we have been given at the ICO from the Data Protection Act 2018 is that we have to develop a code for age-appropriate design. This is a really interesting task because we are looking at the standards of design for kids' websites and games and how companies are going to have to comply with that. We are doing a consultation now to come up with that kind of design. That is going to be unique. That code is unique in the UK and not a requirement anywhere else.

Baroness Bertin: Have businesses been involved in that consultation? Are they running towards it or not?

Elizabeth Denham: The big companies are not necessarily running towards it but they do know that there are special obligations they have to protect children online when it comes to consent and content. That goes back to design. Another principle for the ethical design of internet activities is that people should have the same rights online as they have offline. I am not saying that regulation can be copied and pasted over to the online world but I do think that people should have the same rights.

Q117 **Lord Allen of Kensington:** I am interested in three things. What challenges have you faced implementing the Data Protection Act 2018? Secondly, what are the lessons learned? Thirdly, have there been any common themes? I am trying to get a feel for the level of intervention. Is there a common theme in regard to what has taken up your team's time in the past year?

Elizabeth Denham: Our initial challenge was getting organisations engaged in getting ready for the obligations under the Act. What helped there and focused the attention of organisations on their new responsibilities was the level of the fines. Even though we had data protection law for 20 years in this country it almost felt as if most companies just woke up to their data protection responsibilities when they saw the fines. Data protection becomes a boardroom issue. It becomes a risk issue for senior executives. We spent a lot of time in the last two years both myth-busting about what the Act really required but also helping to ensure that data protection was baked in to the business practices of organisations and not just bolted on in the department of legal compliance. At the end of the day, if personal data is the most important asset that a lot of organisations have, they have to have strong data governance and legal compliance. That was the first challenge—getting the attention of the board.

Lord Allen of Kensington: To specifically pick up on that, the Centre for Policy Studies told us that there was widespread confusion. Do you think that we are through that now? Do you think that there is still confusion in businesses about what we need to do, or is that going to take a number of years?

Elizabeth Denham: We spent a lot of time on guidance and every industry sector wanted their own specific guidance. We have 5 million businesses across the UK and all the public bodies and their special issues and we did what we could. The other challenge was small businesses. Micro-businesses and small businesses were concerned about the new obligations on them and how to identify risks and build in the measures that they needed to. We did a lot of work with industry associations representing small businesses. We had a whole stream of work around small agencies.

There were two other challenges. One was the demand for the expertise of our staff. At one point we lost 25% of our expert staff to other companies that could pay more and attract them. That was a huge impact on the ICO. We might be over that now. The other issue was that we underestimated the exercise of rights. Individuals have come to our office well beyond our estimation. We thought we might have a 30% or 50% increase in complaints and calls and inquiries. It was 100% increase in the first three months under the GDPR. It is crunch time for us to be able to deal with those front-facing services.

Lord Allen of Kensington: What types of incidents have taken up most of your time?

Elizabeth Denham: A lot our time is spent dealing with data breaches. Data breaches and incidents of a significant nature now have to be reported to our office and we had to deal with thousands of those complaints in the first few months. That is liaising with the companies, giving them advice and deciding if we are taking enforcement action, data breach notification incidents and education of various sectors.

The Chairman: You have seen a significant increase in the number of complaints from consumers and from the public. Presumably, you have an investigative threshold by which you determine whether a complaint reaches that threshold for investigation. Do you have any stats on the proportion of complaints that are meeting that threshold?

Elizabeth Denham: Our general process is to require the individual to take their complaint to the organisation first, and only when they are not satisfied with that response they come to us. We get a lot of complaints where people have not taken a complaint to the company or the public body, so those go back and we take the complaints after that. I can write to you and give you a better sense of the numbers that are coming in, which ones we are accepting and even which industry sectors or government agencies they are coming from.

The Chairman: That would be useful if you could write to us. Thank you.

Elizabeth Denham: There has been a 100% increase.

The Chairman: Is your impression that any of those are vexatious or not meeting the threshold and not sufficiently evidenced?

Elizabeth Denham: I think that people have woken up to their data protection rights. We ran a public education campaign called Your Data Matters. That might have been quite successful, but I also think that people are filing more requests to get access to their own personal information. There have been requests for porting data under the new data portability rights. There have been requests for de-linking and removal and deletion of information under their right of erasure.

Lord Gordon of Strathblane: May I suggest something that might save some work? As you allude to in your evidence, most people do not know the terms and conditions that they are signing up to. I freely confess that I am so concerned to put my large finger on the right very small button on my iPhone agreeing to terms and conditions that I do not read them. Would there be a case for your organisation issuing a kitemark, approved stamp of approval, on recommendations so that people know it is safe enough to sign up for this because we all know that nobody is going to read them all?

Elizabeth Denham: That is a great question because I think hardly anybody is reading terms and conditions and there is a lot of fatigue in that approach. The GDPR gives us the ability to certify and to develop kitemarks. That is the next stage of the work that we need to do. I agree with you that people almost need a symbol to be able to identify what is safe and what is not. That will come out of the age-appropriate design code. To start thinking for kids, there almost needs to be a traffic light system.

Q118 **The Lord Bishop of Chelmsford:** I want to ask about algorithms. In what ways do you think algorithms could and should be accountable, fair and transparent? I can say a bit more about what lies behind the question if you need it, but hopefully that will not be necessary.

Elizabeth Denham: One of the reasons that the EU Directive 95 became the GDPR is that there was a lot of public concern about black box algorithms and opaque decision making by machines. A lot of the new rights in the GDPR, therefore, are about algorithmic accountability, about explicability and giving the regulator new powers to audit algorithms for fairness and for transparency. That piece of work is very new to us. If you are asking me how algorithms can be transparent, however, there are different levels of transparency. Consumers need one level. They do not need computer code. They need simple explanations about the algorithms that are at play and, legally, if significant decisions are made by machines with no human intervention they have a right to an explanation.

Another level of transparency is to the regulator. It is for our office and maybe other economic regulators to go in and find out what data goes in, what questions were asked and what are the decisions that come out. That is another layer of oversight. It is not the same as transparency to the people.

The Lord Bishop of Chelmsford: Do you think that the framework that

you now have with the GDPR is sufficient for doing this or would you be looking and hoping for more?

Elizabeth Denham: There may be a gap. The law might sound better than it actually is because it gives the right of explanation to individuals for decisions that are made solely by machines. The wording of the legislation might therefore be problematic. We need time, however, to let the law bed in and to have some cases and to do some guidance and some auditing. The ICO is working with the Alan Turing Institute on a tool for algorithmic transparency and algorithmic auditing. This is a new space for regulators to be in. If there is anything we can do as regulators it is to harmonise our approach to how we are going to look at machine decision making.

Q119 The Lord Bishop of Chelmsford: Forgive me if I was not listening carefully to your answer to the previous question. I was not quite sure if we got an answer to the last bit of the question, but I may have just dropped off for a moment. I was interested in hearing, particularly in relation to this, what the initial lessons are that you have learned from the introduction of the GDPR, because it seems to me that, looking at it not so much with my House of Lords hat on but with my mitre in place as the Bishop of Chelmsford, for the 600 parishes that I serve the anxiety levels were enormously high about things such as, "Do we have to delete our Christmas card list, Bishop?". Now that we have gone through to the other side, I am noticing a huge increase in awareness of these issues, which seems very positive. People's understanding of the world that they have been inhabiting for a while has increased hugely. I think it is the GDPR which to a large extent has done that. It would be interesting, therefore, to hear you reflect more generally on this. The next question might be, as people's expectations are also increasing, how you are going to help them.

Elizabeth Denham: You are right. No pressure for us. There is nothing like a new law to focus everybody's attention, especially a new law with large sanctions—not just fines but also new powers of the regulator that we can order a company to stop processing personal data. This can have more impact than a fine at the end of the day when you think about business models.

Yes, it has focused the attention of companies and public bodies. All kinds of charities are focused on this, with marketing and profiling. I did not like the anxiety, but we kept saying that GDPR was not the Y2K of 2018. It is the beginning of new awareness and better systems in place to take care of people's data. The other thing that is unfortunate is that there were a lot of consultancies that got involved in this and a lot of scaremongering. That is where we had to do a lot of literal myth-busting to say that the GDPR is not all about fines and here is your basic responsibility. If you are a micro-business and you are a butcher on the corner you are probably not going to be impacted by the GDPR.

On lessons learned, I guess we could have tried harder to bust some of those myths earlier, but we had to get the attention of organisations to

do that. We also did not have the capacity to go out and educate every business and every sector.

Baroness Bonham-Carter of Yarnbury: Going back to the algorithms and the risks they pose, one of the things that has come up a lot in evidence given to us so far is the targeting, or micro-targeting, particularly of those with addiction problems and so on. As with the Bishop, you may have answered this in your previous answer, but do you think we have sufficient powers to combat this?

Elizabeth Denham: Yes, we issued a report in July called *Democracy Disrupted?*. That report and our investigation is about the use of data analytics to micro-target voters in campaigns and elections. I would point you to that report because there is a series of policy recommendations in it about improvements that we need in the law. The purpose of the report was to pull back the curtain to show citizens how their data is used in a campaign or a referendum. We are investigating 30 different organisations, from political parties to social media companies to data analytics and political consultancies, to unpack what that ecosystem looks like and why you would get a certain message where that data comes from—data brokers, et cetera. We have taken action against some of those organisations. We cannot do everything under data protection law because there are ethical issues for government, for Parliament and for policymakers to look at, but we are pushing the envelope on that in our large investigation and that is the one that has the attention of the world.

Lord Gordon of Strathblane: The problem is that it is sometimes impossible to trace the source of the intervention. Is the answer perhaps to target the messenger rather than the message and insist that anyone putting something up has to have a real address and be a real person and not a robot and have some process of rectifying the wrong if they have done something wrong?

Elizabeth Denham: Are you talking about anonymity on the internet?

Lord Gordon of Strathblane: Yes, I think that there are issues. Obviously there are arguments on both sides. Some people would not intervene at all if they did not have the guarantee of anonymity but equally I am sure that you would agree that it can frequently be abused.

Elizabeth Denham: That is why I think your job is so difficult.

Lord Gordon of Strathblane: That is why we are asking you to help us.

Elizabeth Denham: You are trying to balance the private space with openness and transparency. If you take a political campaign, for example, everybody agrees, Facebook, Twitter, Google as well, that the source of political advertising should be imprinted. It should be marked and people should know where that ad is coming from. That seems to be easy as opposed to identifying an individual on the internet and what the outcome is of that. These are challenging questions and it will take time for us to map them and identify the significant harms.

Q120 Baroness Bonham-Carter of Yarnbury: I want to come to platform dominance. In your written evidence and in what you have said already today you make it clear that you are concerned about data monopolies. Could the implementation of uniform standards and data portability mitigate what you see as the negative consequences?

Elizabeth Denham: It can help. Data portability is a new right which allows individuals to port their data from one service provider to another. We can see how that might build better innovation and market share so we understand that. It also gives people control. I am concerned about data monopolies, however, when you see for example the spend of political campaigns that goes towards online political advertising, mostly through Facebook, and you think about all of that data in the hands of one company. I worry about data hacks, hacking into a database, and the lack of innovation. I think that is what people are really concerned about, too.

The other thing about data monopolies is that we intervened in a case when Facebook purchased WhatsApp. The purpose of that merger was to share more data. So many mergers and acquisitions that are happening in the market are really about data and consolidating more and more personal data in the hands of the company. In that case, with Facebook and WhatsApp we were able to get WhatsApp to sign a commitment that data sharing would not take place until they could prove to us that it would be legal. Competition law can probably look at some of these issues, but data portability and standards can help.

The Lord Bishop of Chelmsford: Did they prove it was legal?

Elizabeth Denham: No, we are still waiting. Those are the kinds of issues where you see more and more mergers, which are really about getting more data and compiling more data and profiling more people in the commercial sector.

Baroness Bonham-Carter of Yarnbury: You are now fighting it.

Elizabeth Denham: We have not had any more moves from Facebook and WhatsApp on their sharing of that particular data.

Q121 Lord Goodlad: I have two questions. First, what are the problems of enforcing UK regulations on companies based outside the jurisdiction of the European Union—the United States of America being the obvious example—and how are these problems were overcome? Secondly, what effect do you think this country leaving the European Union will have on the overall regulation of the internet?

Elizabeth Denham: How do we enforce UK law outside the bounds of the United Kingdom? We are involved in several cases where we are taking action against companies that are located elsewhere. I will give you one example. In the Cambridge Analytica/Facebook investigation, one of the companies we are investigating, AggregateIQ, is based in Canada. It was involved in the referendum campaign. We are using the help of our Canadian colleagues through a memorandum of

understanding to obtain the information that we need to take action. We have the help of our Canadian colleagues, but the actual enforcement of the law is a challenge. How would we actually carry out an enforcement notice against a Canadian company? That is an open question for us right now. We have taken action against some US-based companies that are associated with UK companies, and by contract the UK regulator has a right to investigate and enforce the law. You will see my decision next week that will make this answer a little less vague. That is by contract.

The GDPR has extraterritorial reach, so it captures the data of EU citizens processed by companies outside the EU. The actual enforcement of the GDPR, however, needs to be given some practical experience and I believe it is going to need bilateral agreements and mutual legal aid treaties—MLATs—to make it real. We are at a very early stage right now.

Lord Goodlad: So it is a big challenge and a big problem.

Elizabeth Denham: It is a big challenge. We will see how practical the extraterritorial reach of the GDPR actually turns out to be in the enforcement. Your second question was about the impact on enforcing the UK law if we are no longer in the European Union. The ICO is a member of the European Data Protection Board, so we have the EU 27 as a strong contingent of enforcement action. If we are no longer part of the board, the UK will be on its own enforcing a similar law but without the co-operation, consistency and mechanisms of the board. If we are not part of the board and there is no data arrangement that keeps us in that enforcement club, we will be turning to bilateral agreements with data protection agencies to do joint enforcement.

Lord Goodlad: Have they been involved in any discussions about this possible eventuality?

Elizabeth Denham: I have been talking to my European colleagues about the eventuality of a different relationship and what that would mean. I know many of my colleagues would be willing to jointly enforce with us. That is very future focused, however, because we do not know what our relationship is going to be right now. It is one for the Government.

Lord Goodlad: Have you talked to the British Government about it?

Elizabeth Denham: I have. I have advised government and been consulted by government on the impact of enforcement if we are no longer a member of the board or part of the European Union.

Lord Goodlad: How has that discussion been reflected?

Elizabeth Denham: In the Government's partnership paper. The Government's ambition is for an arrangement beyond adequacy that keeps the ICO as a member of the European Data Protection Board. If that does not happen we will have to look at bilateral agreements to jointly enforce. There are member states where there is a higher risk to UK citizens where the data is flowing. That is where I would go. My

mandate is to protect the data of UK citizens and I will do whatever I can to have those arrangements in place. I agree with the Government, however, that the best-case scenario is an ambitious data deal that keeps us very close to the Europeans, not just in law but also with joint enforcement. The weather is going to be made in the EU on these big internet cases.

Baroness Benjamin: There is a TED talk by James Bridle, which has had nearly 3 million viewings, called *The nightmare videos of children's YouTube—what's wrong with the internet today*. A lot of the videos that children are watching are not only inappropriate in many ways because of the content but also extremely addictive. I would like therefore to ask you, out of those 3 million people, especially parents, who want to complain but do not know who to complain to, have you had any complaints about this particular part of the internet where children are being attracted to watch inappropriate material? Is this something that Ofcom or maybe the BBFC should be regulating or do we need a new regulator to look at this kind of issue? Do you feel that the regulation of YouTube and other platforms should be the same as for terrestrial broadcasters?

Elizabeth Denham: I am not a content regulator. I do agree with you that in the kind of research we have done with Ofcom about the harms that people are concerned about on the internet, one concern is about children and what they are able to view online, including videos and other sites. A complaint about the content of a video would not come to our office, but I do agree that people do not know where to take their complaints. They might ask YouTube to take the video down, but that kind of issue and complaint is probably better examined by an organisation such as the BBFC, along with some of the filtering and identity. When it comes to addiction online, that is another harm that needs to be carefully identified and scrutinised, but it is not directly a data protection harm. Whether we will be considering some of these issues in our age-appropriate design code I do not know. I am sure that we are going to hear about that in our submissions.

Baroness Benjamin: Do you feel that the organisations that you have already mentioned should all be working together to deal with this type of material, which is online, because there is a world out there that parents do not know how to navigate? Everybody should be getting together because, as far as James Bridle is concerned, we all need to work together to stop children being exposed to online material like this. What would your role be if you had to be part of the bigger conversation?

Elizabeth Denham: If it is part of a bigger conversation, it needs to be because you are talking about many things here, including content regulation, the role of parents and the role of internet companies. It is a conversation that is going on right now. This inquiry is part of that conversation. My response would be that there needs to be a clear inventory of what the harms are, the extent of the existing regulators, what activities they cover, what actors they cover and whether they can

reach into other jurisdictions to have an impact, because many of these companies are based elsewhere. All of these things are important. Only then can you decide whether you need to create a new regulator or add to the remit of the existing regulators.

Baroness Benjamin: They are looking to see how many times the children are pressing the button to look at this material and using it for advertising. It seems to be a link that we have to get our heads around to say that you cannot show that type of thing in order to gain advertising in order to get on to a platform to get to children. It is a sneaky way of getting to children which 3 million people feel is completely inappropriate.

The Chairman: Who would be the lead regulator on the aspect that Baroness Benjamin describes?

Elizabeth Denham: That is a complex set of questions because you are talking about content and also about the use of personal data to target advertising, so that would be my role.

Baroness Benjamin: That is the main thing he was pointing out. The content is just part of it. It is the advertising and getting to the children that people feel is unsatisfactory and somebody should be looking at this because of when the children become teenagers and adults. Eighteen month-old children are getting hooked because of the kind of behaviour that is online. What are we going to do about it? I thought I would ask that question to see where you stand and what you feel that we as a Committee should be doing and looking at.

Elizabeth Denham: There is no silver bullet to say here is the answer, that it should be the ASA and Ofcom and the ISO and industry codes of practice and it should be independently regulated. Those are numerous questions. We are involved when personal data is used to deliver content or deliver advertising. We can look to see whether it was used fairly. For the first time in law in the GDPR, children are treated differently: there have to be special arrangements for children both in terms of the use of data analytics and algorithms but also the form of consent and the use of sensitive data. Children are treated specially for the first time in law in the GDPR. This Committee might look at that, because I do not think it exists in the other laws and regulations. You need another regulator that is deciding to filter certain content or tag it as acceptable or not.

Baroness Benjamin: Could I ask you to look at that video by James Bridle, the TED Talk?

The Chairman: We have taken note of the video you are referring to.

Lord Gordon of Strathblane: I was just wondering, slightly off subject again, whether there is a danger of conflict between the British approach to law and the American approach to law. It has been alleged in written evidence to us that Twitter would disregard a UK court order unless they got a similar one from a United States court. That is an allegation that we

will put to Twitter later in the afternoon, I imagine, but is the difference between American law and British and European law a problem?

Elizabeth Denham: I am not a legal expert in all of these different areas of regulation but, generally speaking, the US is looking at the standards in Europe because they have to look at compliance in a different way because of the jurisdictional reach of the GDPR. For the first time after Cambridge Analytica and Facebook and how data was used during the 2016 presidential campaign, they are looking at these other standards. At the end of the day the approach in the UK has to reflect our cultural values. That is what it is all about. The challenge is that the internet knows no boundaries. Geopolitically the internet does not see that. How do you make sure that British law is respected when you are dealing with large American companies? It is a challenge.

Lord Allen of Kensington: You have talked about a super-regulator—Ofcom, CMA, ASA, FCA or whatever. Have you identified anything that is falling between the cracks? You know what you are looking at. Ofcom is very clear about what it is looking at. I would be interested to know if there is something that is falling between the cracks and, if there is, what we would do about it. There was a suggestion earlier of some sort of co-ordinating body that gets everyone working together.

Elizabeth Denham: There are two things that are falling between the cracks. Although we have defined what illegal content is, people are really concerned that it is not properly enforced online. How do you enforce our standards? If there is illegal content, how do you get it down without depending on companies to be the judge and jury in whether to take that off? When it comes to legal content, where it is legal for the content to be online but it is intrusive or disturbs people or harasses people and does not meet the standard of illegality, who is going to make the determination that that information needs to be taken down or censored in some way? Who makes that decision? That is where you might look at some kind of an ombudsman or an intermediary. You need codes of conduct that are created, certified and backed up by an independent regulator. The space that everyone is grappling with is things such as what do you do with the legal content without leaving it in the hands of the big companies or the platforms. We know they are not just benign platforms any more, but what is their responsibility and liability?

The Chairman: Thank you very much for your evidence, which has been very impressive and informative for the Committee. Thank you also for the written evidence that you sent us. We have had a very interesting discussion about the possible need for an overview across the regulatory piece and some of the potential gaps that you have identified, some of which Parliament may feel are not being addressed by regulators. It may well be that as we develop our thinking on that we may want to come back and talk to you further. Your evidence in that area has been very interesting, as has all of your evidence. Thank you for your time today.