HOUSE OF COMMONS

Digital, Culture, Media and Sport Committee

Oral evidence: Fake News, HC 363

Tuesday 6 Mar 2018

Ordered by the House of Commons to be published on 6 Mar 2018.

Watch the meeting

Members present: Damian Collins (Chair); Paul Farrelly; Simon Hart; Ian C. Lucas; Christian Matheson; Brendan O'Hara; Giles Watling.

Questions 849-942

Witnesses

I: Bill Browder, founder and CEO, Hermitage Capital Management, and Edward Lucas, Senior Vice President, the Center for European Policy Analysis (CEPA).

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

Written evidence from witnesses:

- Edward Lucas
- Elizabeth Denham, Information Commissioner

Examination of witnesses

Witnesses: Bill Browder and Edward Lucas.

Q849 **Chair:** Good morning, Bill Browder and Edward Lucas. Welcome to the Committee. My apologies for the slightly later than normal start this morning. Starting off with you, Mr Browder, our interest in calling you in front of the Committee is as someone who was a personal victim of fake news and disinformation emanating from Russia. Perhaps you could start off by telling the Committee a little bit about your personal experience.

Bill Browder: Sure. My name is Bill Browder, and in spite of my accent I am a British citizen; I have been living here for 29 years. For 10 of those 29 years I spent quite a bit of time in Moscow, running the largest investment fund in Russia. It was called the Hermitage Fund. I discovered, among my investments, that many companies were being looted by corrupt Government officials, and I thought the best way of dealing with the looting would be to expose those officials through the media. I ran what were called "naming and shaming" campaigns.

As you can imagine, that did not end up being too popular with Vladimir Putin, and in 2005 I was expelled from the country and declared a threat to national security. My offices were then raided in 2007 by the police, who seized all our documents. I hired a young lawyer named Sergei Magnitsky to investigate the reason for the raid. Sergei investigated it and discovered that the purpose of the raid was ultimately to steal $230 million of taxes, which my firm had paid to the Russian Government, from the Russian Government through a complicated scheme—I will not explain it unless you are interested, but I am happy to do so if you are.

Sergei discovered this theft, which was not from me but from the Russian Government, by Russian Government officials, using my documents and so on. He exposed this theft and, in retaliation for exposing the theft, Sergei was arrested by some of the same officials he exposed. He was put in pre-trial detention. He was tortured for 358 days and he was killed in custody by eight riot guards with rubber batons on 16 November 2009. Since then, I have been on a campaign to get justice for Sergei Magnitsky. My campaign to get justice for Sergei Magnitsky basically brought me into conflict with their campaign to make sure that I did not get any justice.

Their campaign to make sure that I did not get any justice was first of all to change the narrative of what happened to Sergei. We have an absolute mountain of documentary evidence that Sergei was beaten, including photographs of his body, and autopsy reports saying that there were various injuries to his head and other places. The Russian Government, on an official basis, through all sorts of different high-level officials, said that Sergei died of natural causes, he died of heart failure and there were no

signs of violence. Then they repeated it over and over again at every different level of the Russian Government, going right up to Vladimir Putin.

The Russian state television got involved in basically changing the narrative, and then, as I went on a campaign to get justice, they started to go after me and Sergei. They then accused Sergei of various crimes and they put Sergei and me on trial, three years after they killed Sergei, in the first ever trial against a dead man in the history of Russia. Afterwards, the Russian authorities started to use all the different arms of the propaganda machine to try to change the narrative about what happened, outside and inside Russia. They made six movies about me, in which they claim that I am a serial killer, an MI6/CIA operative, a tax cheat and a swindler, and that I stole $4.8 billion of IMF money headed to Russia. They have repeated those allegations in an official capacity, on television, on Twitter and Facebook and by every other means.

I was pleased to be invited to discuss my experience in front of this Committee, because I have first-hand experience of how this all works, what their methods are and what types of things we can do to stop them. I don't want to spend too much time talking, because I know you will have questions, so I will stop my introduction there and let Ed talk as well, or however you want to do things.

Q850 **Chair:** Thank you for the introduction. I will follow up and ask you to tell the Committee a little bit about how disinformation campaigns against you are waged, and how they manifest themselves. This Committee has had the pleasure of being simultaneously attacked by both the Russian Embassy and Breitbart on social media for our inquiry, which shows we are doing something right, but I am sure that is on a smaller scale than what you have had to cope with.

Bill Browder: One of the big misconceptions of fake news is that it is somehow just a technical issue surrounding social media platforms. There is a huge technical component to the fake news issue—that Twitter, Facebook and Google are all being used. I will explain how they are being used in a second, but in order to do this whole fake news thing, it all comes back to a source, and the source is the Russian Government and high-level Government officials.

One of the most important things to understand is that it is very difficult for anyone in the West when they hear an official—the General Prosecutor, Prime Minister or President of Russia—making statements that are outright lies. That's the crux of the problem; then the problem of those outright lies gets disseminated across all of these different tools.

So we will have Vladimir Putin saying that Sergei Magnitsky died of natural causes—that he wasn't murdered. That will then be repeated by the Russian media; it may even be repeated by certain Western media sources. Then those Western articles will be put on to Twitter, and Russian bots will then repeat those same statements in thousands of different places. That will then be put on to Facebook, and then my Wikipedia page will be attacked and all sorts of people will link my Wikipedia page to all of

those sources. They don't necessarily have to convince everybody that they are right; all they are trying to do is convince everybody that I am not necessarily right. The purpose of Russian disinformation and Russian propaganda is to plant a seed of doubt in everybody's mind. If they can create that kind of confusion, they have accomplished their objectives.

Q851 **Chair:** May I ask one question? Perhaps Edward Lucas will want to comment on this as well. There has been a lot of analysis on Russian agencies involved in disseminating fake news, particularly agencies like the Internet Research Agency. We have received evidence discussing whether there is co-ordination between agencies that disseminate fake news and hyper-partisan news agencies, like RT and Sputnik, that then amplify the Russian world view. Do you think that, for campaigns to be effective, it requires the support of actors within a country like the UK; it can't just be done by firing information in from the outside?

Bill Browder: It is all part of the ecosystem. If it were just from the outside, it would be less effective than if they can create some type of support from the inside. They get support from the inside in a lot of different ways. You have mentioned certain media organisations which help them do that, and it does not look like a foreign activity. If Sputnik News or RT generate something, everybody looks at it—or most people look at it—with some question. You mentioned Breitbart; if they put something out which mirrors that, that's a domestic media organisation so it couldn't possibly be a foreigner.

Then they also have what I call agents of influence. They find people—an American or British person—who may be paid, or might just have a philosophy or personal motivation that is different from ours, who can go on TV and support that view. For example, today we are all sitting in the middle of this incident in Salisbury. I was on "Newsnight" last night, and there was a person who was taking the other side of the position. They were basically spouting a completely inappropriate, Putin-apologist view of what was going on with Russia. They were saying that we should not make any assumptions whatsoever: there should not be any kind of alarm about what was going on in Salisbury. It was probably a person who was just ideologically in a different place, but they found that person and that person was on RT yesterday, and on all the UK media, basically spouting the Russian position.

We have this whole concept of media fairness. Ed and I were talking about this in the hall before the Committee sitting. The BBC feels compelled to say that the round-earth people and the flat-earth people all should have their say. There are some things where you don't have to get the say of the pro-Putin people on television here—to give them equal airtime.

Edward Lucas: I think Bill has put it very well. We are essentially a very fair-minded and trusting society. We assume that in most disputes there will be two sides to the coin, and that they both deserve a hearing, and we assume that people in the public space are broadly telling the truth, and even if they are not actually correct, at least they are saying something

that they believe is correct. That gives Russia and other hostile actors room for manoeuvre.

I don't know whether you heard the "Today" programme this morning, but we had Heidi Blake from BuzzFeed talking about her investigation, which showed there have been 14 mysterious, suspicious or unexplained Russia-related deaths in this country since 2006. She was up against the deputy editor of RT, the former Russia Today, who was basically just spraying doubt over the whole thing, saying, "How can you be really sure?"

We had this when the Home Secretary—I think it was the Home Secretary, or maybe the Defence Secretary who talked about the Russian cyber-attacks on this country and how serious they were. I was on "Newsnight" with a Russian journalist who, again, just said, "Where's the evidence? What's all this about?"

It is a legitimate subject for journalistic inquiry—what is Russia saying about this?—in the same way as we would analyse jihadist propaganda. It is useful to know about; we inform the public about it. But we should not put that on the same level as the very serious question, "What is going on, does it matter and what are we doing about it?" Those are the three elements, or should be the elements, of our national security strategy when dealing with Russia, and I think we are failing on all three of those. We have not really got a picture of what is going on; we have not worked out which bits of it matter; and we have not worked out what we should be doing about it.

Q852 **Chair:** A final question from me, Edward. Do you feel that there is enough seriousness within the intelligence community in Western countries to look at disinformation as, effectively, a weapon that has to be countered, or has the priority been laid more on defending public institutions from more direct cyber-attacks?

Edward Lucas: I think it varies very much between countries. Our allies in the Baltic states, Poland and the Czech Republic probably know more than we do on some of this stuff, and the Swedes and Norwegians are also very good. There are other parts of Europe where the awareness and capability are very limited.

But I do think it is important—I think I have made this point to you before—not to look at information operations in isolation. Information is just one Kremlin tactic. We may have seen in Salisbury this week another tactic, which is physical intimidation or elimination of opponents. There is also the cyber stuff, the abuse of the legal system, which Bill Browder has experienced with the use of red notices, and which Chris Steele, the former British official, is experiencing with the mendacious lawsuits that he is facing. They have all these different tactics. Some of them will have no information dimension; for some of them, the information dimension is the main one. But we should never make the mistake of thinking the bit of the problem we can see is the bit of the problem that we most urgently need to deal with. It may be in some cases that the information dimension of

these operations is a distraction and what matters far more is the money, for example, or some other thing that is going on.

Q853 **Christian Matheson:** Mr Browder, a quick question, in the current context. Do you ever fear for your own personal safety?

Bill Browder: I do. The title of my book is "How I Became Putin's No. 1 Enemy". It's sort of tongue-in-cheek, but at the same time it's very real, in the sense that I have been threatened. I have been threatened on a number of occasions with death, including by Dmitry Medvedev, the Prime Minister of Russia, at the World Economic Forum in Davos. When a group of journalists asked him about Sergei Magnitsky, he said, "It's a shame that Sergei Magnitsky is dead and Bill Browder is still alive and running around." I have received kidnapping threats. That is on the unofficial side. On the official side, what the Russians would like to do with me more than anything would be to arrest me, get me back to Russia and then kill me within the control of their own system. So, as Ed mentioned, I have been the subject of six Russian Interpol red notices and the British Government have been approached 12 different times for mutual legal assistance from Russia, including my extradition. Russia has gone to a number of other countries: I was recently detained in Switzerland, based on a Russian information request at Geneva airport.

I am at high risk. I don't spend my life living in fear but I am definitely at risk.

Q854 **Christian Matheson:** May I ask you both about Russian—or other—interference in democratic elections: the elections in the UK, the referendum on the EU? We heard from Facebook that they felt that there had not been very much Russian meddling at all in the EU referendum and they had done some quantification of what they thought the Russian meddling was in the American presidential elections. What is your assessment—both of you might want to answer—as to the extent of interference in domestic elections?

Edward Lucas: One of the problems is that this is something we should be able to get empirical data on and we can't because we do not have the co-operation of Facebook. We need to know who, in political speech, is regulated in our country, and quite rightly so. As you all know from your own elections, you have those "printed and published by" documents and it is an offence to hand out anonymous propaganda in an election. Facebook is a vehicle for anonymous propaganda and we are not getting the help from Facebook. I think your Committee grilled Facebook representatives on this.

One very important starting point is that we need transparency about advertisements on all the communication service providers, chiefly Twitter, Google and Facebook. It should be possible, if we see an advertisement, to find out who has paid for it. We should also have some idea of who has seen it and who has clicked on it. Facebook always plays the privacy card—I don't know if there's anyone from Facebook behind me furiously taking notes, but I am sure they would love to make the point that people

have the right to privacy. I think once you engage in advertising you basically give up your right to privacy. It is almost like an opposite. Particularly if it is political advertising, you can't expect to have the right to privacy. If we could find out what was going on with advertising, that would give us a very good clue as to where Russia and other hostile adversaries are putting their money and efforts. It may well be that Britain is not a priority—maybe they are targeting some other country. At least we would know.

There is a second very important point, which is about propagation. We need to know about realness. We need to know whether the accounts where people are just sharing as opposed to advertising, but behaving as individuals—we need to know whether that is a real Twitter account, a real Facebook account. As I showed in my written evidence, it was extremely easy for me to set up not only an email account in the name of Mr Collins but also a Facebook page in his name and a website in the name of this Committee.

Chair: If you want to come and help the IT support, you are more than welcome.

Edward Lucas: This is trivially easy and once you do it—and there may be good reasons for doing it: you may be doing a human rights campaign or something where you need to stay anonymous—there is no way of telling. At the moment, it is very hard to tell if this is real. We need that data from the communication service providers about realness. And if we have that, we would then be able to say, "Isn't this interesting? Here are 25,000 Facebook accounts that have no realness: they do not have phone numbers, they do not behave like real people. They are the ones pumping out propaganda on one side or another of an election or Russia and so on." Then you would have idea, but at the moment we have no idea.

Q855 **Christian Matheson:** Facebook wrote to the Chair on 28 February stating that in their investigation, which I think they had undertaken to carry out at the behest of this Committee, that they had found no additional co-ordinated Russia-linked adverts in the UK regarding the EU referendum. By the sound of things, you are not quite convinced that this is accurate.

Edward Lucas: I don't think Facebook should be in a position of marking its own homework. They have a duty as a platform to have transparent rules that can be discussed with the outside world and we should be able to check stuff. It may well be—I don't exclude the idea at all—that Russia looked at the British or Italian or German or French or whatever elections and said, "These guys are screwing things up so we don't need to intervene." I am not saying that the Russians are behind everything that happens, but they are behind some things. We know that they have intervened on some things, such as the American election, and that, to me, is already evidence enough that we cannot just trust Facebook to go after the event and say, "Nothing to see here, move along." We should be able to see in real time who is advertising.

Q856 **Christian Matheson:** Aside from Facebook and the other platforms,

Twitter and Google and so on, what other indicators should we be looking for in terms of seeking out evidence of foreign interventions?

Edward Lucas: I think there is advertising, which I have already mentioned. That is the first thing. The second is what is sometimes called computational propaganda—using the power of computers to make things happen. That would be trolling with bot accounts, so it is not real people but either computers being programmed to do stuff or people being paid to do stuff. Once you have identified those accounts you then need to say, are they introducing new ideas, wrong ideas, into the debate—so, for example, claiming that something has not happened when it has happened, or spreading a scare story or hoax, or something like that.

You could also look at application, where they are taking something that is essentially marginal and making it into a big deal. You can do this on Twitter quite easily. You can just hire millions and millions of bot accounts to make something trend, and when it trends people look at it. For example, in the Scottish referendum—and we have very good evidence on this—the Russians sowed seeds of doubt about whether the referendum was fair. We have never had that in this country before. We have all sorts of disagreements about our politics, but no one has ever—not since, I think, the 1830s has anybody really had the idea that we stuff ballots, or don't count them properly. We are always pretty good at doing this. Yet we saw, after the independence referendum in Scotland, the Russians pushing out the idea with pictures of ballot boxes and votes being moved around, saying, "This is being rigged." That had an effect on the public. There are still people who believe it. The Scottish nationalists, who had every interest in it—if there had been anything going wrong, you would have shouted about it. You would have said, "Hey!" There was no complaint from any representative of the losing side in the referendum that anything had gone wrong. This whole thing was manufactured on social media and it had an effect. That, to me, is the No. 1 evidence of interference.

Q857 **Christian Matheson:** Finally, if I may: there seem to be two schools of thought, depending on where your own political views and prejudices are. Whether we take a general election, whether we take the Euro-referendum, there are those who are happy with a particular result and say, "Look, we have seen the evidence. Nothing to see here," and there are those who might think, "The Russians have meddled elsewhere; they have meddled in the United States"—and there is evidence you have just given us of meddling in the Scottish independence referendum—"It stands to reason, therefore, that they would probably be meddling in the UK general election and in the Euro-referendum." But there still seems to be a lack of conclusive evidence one way or the other.

Edward Lucas: I would be cautious about this, actually. I do not think that there is evidence that they particularly push—one might have assumed they would try and push the Scottish independence cause, but there is not strong evidence of that. I think what they were trying to do was to cast a doubt and to corrode public confidence in the integrity of the system itself, in this case, by casting doubt on the fairness of the count. I

would not want to win an election, or my side to win an election, with Russian help, because I would feel it contaminated the integrity of the result, and because the next time the Russians might be on the other side and use it against me. We do not want outside interference in our politics whether it benefits us or hurts us. It is wrong in principle.

Q858 **Ian C. Lucas:** You slightly touched on this already, but you mentioned that Facebook responded to us about advertising from Russia in connection with elections in the UK; but it is not just about advertising, is it? You mentioned bots and individuals who are paid to work on social media. How are we going to be able to assess the influence of that? What can we do to find out whether this is actually happening?

Edward Lucas: I will submit some more detail on that in a written answer, because it is something I have thought about a lot; but I think the first thing we need to do is to get away from the idea that anonymity is the default setting. It should not be possible that you can set up a website and a social media or email account, and behave as if you are real, with no way for people to find out that you are not real. We need a different system of identifying where we are on the internet and who we are dealing with. That should be an opt-in system rather than being compulsory. We sort of have that with Twitter at the moment, where you have a blue tick. You kind of know that if someone is tweeting as the Department for Digital, Culture, Media and Sport Committee with a blue tick, that means that someone from Twitter has taken the trouble to make sure that it really is that Committee, and that it is not a parody account set up by your rivals in some other part of the system.

We need to build on that. We need ways in which you can sign something to say, "This really is Ian Lucas MP writing to you," not just someone who has set up a gmail account saying "Ian Lucas MP". When we go to a website, it will have a security certificate: "https" means that someone bought a security certificate and installed it, and that means that the traffic from your computer to that website is encrypted—it gives you some protection against some sorts of cyber-attacks. The security certificate should also give some idea of realness—of identity—for example, that this person has a phone number and gave one when they set up the website, that they have a bank account, that they have a street address—all these different things, which we absolutely expect when we are dealing with people in the real world. When the internet was set up, nobody ever said, back in the 1980s, "Guess what: we are going to have the central nervous system in one civilisation and we are going to use this for all our financial information, entertainment, infrastructure—everything. We are going to make it almost impossible to know if the person you are dealing with is real. Isn't that a great idea?" We would have thought that was crazy. When the motor-car came in we very quickly decided that cars needed number plates. Planes need number plates, ships need flags: we are quite used to the idea that you need to signal realness—to give data to the people who are dealing with you. We should have the same sort of thing on the internet.

Q859 **Ian C. Lucas:** What about the argument that removing the anonymity

would, in certain regimes, remove a powerful advocacy of free speech?

Edward Lucas: I am not against anonymity, but it should not be the default setting. I would fight to the death to preserve the right of people to be anonymous if they wanted to. You should be clear that when someone is anonymous they have chosen that, and that there must be a good reason for it. It might be Chinese human rights or Tibet or Chechnya or something like that, and then people would say, "Fine, obviously that is going to be anonymous." But there is no reason why the DCMS website would be anonymous, and that should be a glaring red flag that something is wrong.

Bill Browder: I just wanted to say that one has to look at the financial motivations of these companies. Twitter and Facebook make money by having lots of users, and it is not in their financial interest to self-regulate or to give you the most frank assessment of what their role has been here or elsewhere.

I cannot comment on Facebook's answer to your question because I do not know what they said here, but Twitter was brought before Congress in the US. Their first response on Russian interference was to say, "Yes, we have identified 200 accounts that might have been connected to Russia." I laughed when I saw that, because I can find 200 accounts in the last hour from Russia dealing with me. Eventually the number went from 200 to 2,000 to 20,000. But the point is, as Ed said, that you cannot have them marking their own homework.

It is all about money. These companies are some of the most important, financially valuable institutions in the world. They are also afraid of losing money. When I was invited to come here, I was asked what kind of recommendations I could make, and the one thing I would say is that if BP is making lots of money pumping oil in the Gulf of Mexico, and then one day they do something wrong and oil spills everywhere and ruins the fish and the beaches, they have a financial liability. We have a comparable situation here, whereby Facebook, Twitter, Google and other companies have been used, effectively, by a rogue regime to create chaos in America and other places. At the moment they bear no responsibility. There should be some financial responsibility.

You are trying to figure how to police Facebook: we do not have to police Facebook if you create a financial liability in the same way as banks face a financial liability if they launder money. If regulation is put in place that creates a financial liability to social media companies that allow themselves to be used to disseminate malicious information, they will police themselves. They know better than anyone how to police themselves; they just have no financial incentive to do so at the moment.

Q860 **Ian C. Lucas:** Twitter admitted in evidence that they gave to us in the United States that they had detected efforts to engage in elections in either the US or the UK by two different organisations, which, interestingly, were Russia Today and RT America. We know therefore that they can do it. What you are saying is that they need to try a bit harder.

Bill Browder: In terms of identifying who is doing this? I can identify who is doing it today. Just today there is a big debate on Twitter about the Salisbury incident. You can tell where the other side of the debate is coming from, so there is no mystery to this whole thing. As Ed said, if somebody can set up 10,000 fake accounts on Twitter and then press a button and disseminate all sorts of fake information, and there is no person behind that, who should bear the responsibility of that? Twitter should bear the responsibility of that.

Edward Lucas: There is a dirty secret that these companies are sitting on, which is that so many of their accounts are fake. I think estimates are that between a fifth and a tenth of all the accounts on Facebook are not actually linked to an individual person. That is quite bad for business. But we have to hold them to account.

I slightly disagree with Bill because I think policing content is very difficult. We have already seen this with the child abuse images that Facebook was taking down—famous photos, pieces of well-known art and so on. Going after the identity assurance of the people behind the accounts is the way to go. If you strip out the anonymity, it would then be much harder for the Russians, or indeed anybody else, to push these messages without it being very conspicuous.

Q861 **Chair:** Mr Lucas, on that point, couldn't you say that if it is true that between 10% and 20% of accounts on platforms like Facebook and Twitter are fake, and yet they sell advertising against those accounts, that is basically a form of fraud? We should be asking the Competition and Markets Authority to investigate the mis-selling of advertising.

Edward Lucas: The advertisers are very interested in this and would be very keen to know. Once you get some data about realness, everything starts changing. Advertisers will say, "I will pay you more if the advertisement is seen by someone who has a 10 out of 10 realness score than if it is only a 1 out of 10 realness score." You create a whole ecosystem in which the authenticated identity is right at the top and the anonymous ones are pushed to the margins.

I agree the whole thing is kept afloat by advertising, fundamentally, and we should never forget that we are not the customers of Facebook; we are the product—they are selling our attention to the advertisers.

Chair: Exactly, it is free—you are the product. That is the rule of thumb. Giles Watling and then Paul Farrelly.

Q862 **Giles Watling:** Mr Browder, your evidence earlier is frankly quite chilling. I don't want to alarm you in any way, but we have the examples before us of Giorgi Markov and Alexander Litvinenko—people like that—and we don't empirically know who carried out these atrocious acts. You say you are enemy No. 1. I want to ask you this very straightforward question: why do you think you are still here?

Bill Browder: That is a good question. I believe that they want to kill me, but they want to kill me and be able to get away with it. If they kill me in

a very brazen way and they don't get away with it, then there would be big repercussions. They haven't figured out a way yet to kill me and get away with it.

Q863 **Giles Watling:** I was just wondering, is it not possible that they want to use you in some way? In some ways you are more useful as you are, doing what you are doing. Perhaps they can use you in some other way.

Bill Browder: I think Ed would probably agree that I am such an irritant to them that that is probably not the reason I am still here.

Q864 **Giles Watling:** Thank you. Mr Lucas, in the evidence you gave in November 2017, you said that fake news has been around since we started chatting over the garden fence. But when we were chatting over the garden fence, we knew who that strange character was in the village who maybe held odd views, and that was quite containable. Do you believe that it is the length and reach of social media platforms now that potentially make this so dangerous?

Edward Lucas: Yes. I think that the internet has added ubiquity, immediacy and anonymity to what was already an existing problem. If you cast your mind back to the cold war, the Soviet Union ran disinformation operations through a mixture of useful idiots, the telex machine and short-wave radio, using dodgy outlets in dodgy countries.

Now it is much easier. You can set up a website that looks like an American newspaper. You can do it totally untraceably; you can use your state intelligence service to steal material and then you can leak it on that website. That is exactly what they did with DCLeaks and USA Politics Today—two of the sites used to propagate the stuff that was stolen from the Democratic campaign, which was leaked in a way that distracted and damaged Hillary Clinton.

That would have been far harder to do during the cold war. They would have had to break into the campaign and physically steal files—we know from Watergate that that is quite tricky. And then how would they get them out to the public? Now you can do all that without leaving Moscow—simply from your keyboard. That is a qualitatively new dimension to this, and you are quite right to put your finger on it.

Q865 **Giles Watling:** And very powerful.

Edward Lucas: It is asymmetric. It gives the weaker party the chance to do things to the stronger party, which it would not be able to do otherwise. In a way, it is harder for us to do that to them than it is for them to do that to us.

Q866 **Giles Watling:** I was going to ask you about that. Have you seen any evidence of it working the other way?

Edward Lucas: I think there are things that we could do, but we are quite constrained. On the whole, our western intelligence services have to meet tests of proportionality, legality and so on and answer to democratically elected politicians, not least your counterparts at the ISC.

I heard it put very well: the Russian security culture is like a jam session: people try something, and if everybody likes it, they pick up the tune and it goes on for a bit. But it is not structured in the way that our set-up is, so you can have things that, if they go wrong, are dismissed as rogue operations and no harm is done. If they work, it becomes a thing.

A lot of these hacking and leaking attacks started off as experiments, and when they worked, they did more of them. When they stop working, they will stop doing that—and to a large extent, they have stopped. They are now developing new things. I commend it to the Committee to please not spend too much time looking through the mirror at what Russia just did to us. Please look through the windscreen at what is coming down the road, which I think will be much more difficult and dangerous than anything we have experienced so far.

Q867 **Giles Watling:** Going on to Twitter specifically, on 8 February we took evidence from Twitter and they denied responsibility: they provide the platform, and people can say what they like on it. There is the First Amendment—freedom of speech—so people can say what they like, so Twitter have no responsibility. One thought occurred to me, which we have talked around so far, which is, do you believe that platforms such as Facebook and Twitter should have a kind of health warning: "What you see here may not necessarily be true"—that sort of thing?

Edward Lucas: Yes, absolutely. If you imagine an airline that said, "Our job is just flying planes around. It is not up to us who gets on to the planes," we would say, "That is a very interesting idea. You cannot land at Heathrow though." These companies operate in a law-governed space; they benefit from the fact that they operate in a free, legal society. We have the right to ask them to be more transparent and to co-operate with research requests. I have not mentioned those so far, but it is very important not to make this into a tussle between the state and the companies. We should be saying to the companies, "Open yourselves up to academic, NGO and third-party scrutiny," because you are much more likely to find mistakes happening if you have the Bill Browders of the information world looking at you than if it is simply a question of box-ticking by some Government agency.

So there is an awful lot that we can do. We just have to fundamentally say to these companies, "Stop being so arrogant. Stop being so complacent. Understand that you are now an extremely important part of modern life, and that brings with it really important responsibilities, so please face up to them, and let's start a conversation about how you can match your commercial obligations, with what you might call your public hygiene ones."

Q868 **Giles Watling:** Can I ask one final question on that? I got the impression when we interviewed people at the hearing that a lot of these companies were being brought blinking into the sunlight—they hadn't seen this coming. To a certain extent, they created the platform, they created the magic and they created what they believe is a great tool for democracy—and we saw examples of that in the Arab spring—but they did not see

what else it could be used for. Do you think that is the case?

Edward Lucas: Absolutely. I think they were run by engineers, who were brilliant with computers and had very little idea. In my own experience, I have met people at these companies who barely understood the difference between civil and criminal prosecution. They are people who are absolutely ignorant of geopolitics. If they thought anything, they thought Edward Snowden was a hero and the NSA was bad, and that was probably the end of their thinking about this. I think that, within these companies, there is quite a tussle between the people on the security teams, who often come from Government, or that sort of world, who see these things happening, and the people who run the companies, who typically say things like, "Where's the data?" You come up with some examples, and they say, "That's just anecdote. I want data." Mr Zuckerberg himself, with grotesque complacency, dismissed the idea that anybody could be using Facebook for political means. Now he admits it's a problem. We should encourage his education further.

Q869 **Paul Farrelly:** Mr Browder, can I first salute your courage? I was a journalist many years ago and was involved in a number of investigations into corruption and money laundering in Russia, in the days of the Wild East. For that reason—then and to this day—I am wary of visiting Russia. So what you are doing is amazing. In terms of social media, has it been your experience that fake accounts have been created to masquerade as you, to try to discredit you? If so, what has your experience been of dealing with social media companies to ask for those to be taken down?

Bill Browder: That is a good question. It has been pervasive on Twitter and on Facebook. On Facebook they not only put fake Bill Browder accounts up, but they then started engaging with people who are my supporters or friends and making all sorts of inappropriate statements, fighting and so on. I get letters and emails from people saying, "Is this really you? Did you really say this?" I wrote to Facebook, and it did respond immediately and take those down.

It is a little more problematic on YouTube, which is a Google company. The Russians make a lot of movies about me. There are a number of official movies from the Russian Government and then there are a number of unofficial movies. Some of that stuff gets taken down if it violates copyright or there is something clearly over the line—if they are inciting violence, which in some cases there is—but a lot of the stuff they do not take down, and that stuff remains.

Q870 **Paul Farrelly:** So, on accounts masquerading as yourself, you have had pretty prompt responses.

Bill Browder: On accounts masquerading as me on Facebook, we have had a prompt reply and a prompt shutting—

Q871 **Paul Farrelly:** And Twitter as well?

Bill Browder: Twitter is a little more complicated, because they allow parody accounts and so on. My account has a blue tick, as we were

describing, so everyone knows that it is me. However, there are all sorts of accounts with my picture on them where they are faking.

Q872 **Paul Farrelly:** So the experience has been variable.

Bill Browder: It has been variable.

Q873 **Paul Farrelly:** Do you think that Facebook has been prompt with you because you are very high profile?

Bill Browder: I am sure everybody is prompt with me. Interpol is prompt with me, because I am high profile. I do not think I am a good case study in how well these organisations are dealing with it. I am a public figure in this campaign, so I do not think we should use that to let them off the hook.

Q874 **Paul Farrelly:** But I imagine your enemies are always trying this on, because it is the old Ho Chi Minh tactic of keeping you looking over your shoulder and tying you down.

Bill Browder: Well, as Ed said, it is this whole jam session thing. When there is no accountability in a Government, they can literally try a thousand different things. They can spend money on a thousand different initiatives, and no one gets in trouble for 999 of them failing and for spending money on those failed initiatives if one of them gets through. They are coming at me with every different method, hoping that just one of them works or has some effect.

Q875 **Paul Farrelly:** I have had one particular case of impersonation driving one of my constituents crazy, with nothing happening. If you go to the police, with the resources they have—these things are often offshore—and you cry identity theft, you get no real response. Have you dealt with the law enforcement authorities? What co-operation have you had from them?

Bill Browder: I don't have anything good to say about the law enforcement agencies in the UK in relation to Russian activities up to and including murder. We had a terrible incident where a man named Alexander Perepilichny—he was a whistleblower who came to us with information about Magnitsky's murder—dropped dead out jogging in Surrey. The police to this day refuse to investigate it. They qualify it as a non-suspicious death. If that is what they do with a Russian murder, when it comes to impersonation on Facebook I can guarantee that there will be no response.

I do not think it has to be an authority thing. If real liability is created for these companies, it can be done on a civil basis by people who have been victimised. If Facebook is worried about their civil liability, they will quickly shut down that account or create a mechanism. It is absolutely all about risk-reward. If there is a risk to them from misbehaving or allowing their platform to be used for misbehaviour, they will stop it themselves.

Q876 **Paul Farrelly:** And we see what has happened in Germany about hate crime. For the record, which force was it?

Bill Browder: The Surrey police force.

Q877 **Paul Farrelly:** Mr Lucas, you raised an interesting point about rights to privacy. My question is about how you think Facebook balances rights to privacy. We have just been to the United States, where people have fewer rights than over here in terms of data protection. I have not tried this, but I think I should have the right to find out why and how a particular dark ad appeared on my account and might be appearing for me as against someone else of similar views—it might be because I am more valuable. I do not know what the response would be. It might be, "Like ITV, we use these ads to pay for a service that we give you for free, and you can always not use our site." How do you think Facebook balances rights to privacy, beyond using that as a slogan?

Edward Lucas: I think we are entering a very confusing new world where a lot of our traditional ideas about privacy will be tested. One is the point you have just made that there is an extremely useful service that you basically pay for by sacrificing your privacy. There are questions then about how much you should know about what you have done. Do you have the right to see all the data that Facebook has collected about your preferences that helps them sell ads? How should that data be provided? I am in favour of the Estonian approach that the individual owns all of the data about them, but that is one case where, with the GDPR coming in—we are assuming that Britain sticks with that data protection regulation after Brexit—there will be a lot to talk about.

I think there is a more difficult question about tagging, and this is where our old thinking about privacy just turns on its head. If someone takes a photo of you, you have no consent over that photo being taken, and it is hard to see any regime in which you could require the person taking the photo to get your consent. That photo goes up on Facebook, someone tags it with your name and it is a public post. Everybody in the world who looks at that will know that you were in the company of those people at that place at that time, and your ability to mingle anonymously with the crowds has gone forever. That is a huge problem, not least for our intelligence agencies. The idea that you can be just a face in a crowd is rapidly going as a result of the constant picture capture that is going on all the time and the ability of computers to turn those pictures into numbers, locating them and correlating them with identities. I have just read a book about this so I am very conscious of it, but I do not have an answer to it.

Q878 **Ian C. Lucas:** If I can just interject slightly, that is only if we know the picture is real, which is another problem. Some of the evidence we heard in the United States was that things like voice recognition and photographs were at such a stage that it is becoming very possible to manufacture images like that.

Edward Lucas: It goes both ways. You can't tell whether an image is real, but people will still draw conclusions from it as if it were real.

Q879 **Paul Farrelly:** I think you have answered the obvious follow-up question to that with a non-answer. I don't use Twitter—I don't look at it—and I've

largely stopped using Facebook now, because I find it an abusive space, but even if I were to stop using it, it wouldn't stop people doing exactly what you are saying in terms of tagging, which is a particularly annoying feature of it, so I just don't look at it. So what answers could there be?

Edward Lucas: I think, in the end, what we are going to need is a way of signing pictures to show that we agree that they are real. So if I take a picture of you and you sign it with your cryptographic signature, then anyone looking at that will see your public key and say, "Yes, that really is Mr Farrelly—he agreed to that." If I am a reputable photographer, I can sign it too—say it was the BBC or some other news outlet—so people can look at an image and say, "This image at least has the backing of a reputable platform and the individual concerned." Other images may or may not be true, but they are basically like cartoons: you don't necessarily ignore what is in them, but you won't have the same level of realness. But we are miles away from having distributed public key infrastructure of the kind that we would need to make that happen. This would work fine in Estonia, but I cannot think of any other country in Europe where it would work.

Q880 **Paul Farrelly:** My final question gets to the issue of the extent to which these are neutral platforms or publishers. At least with certain types of photographs there is an editors' code in newspapers governing what is right and what is not right to publish, particularly with young children. How do you feel about this issue of whether more steps are needed, either externally or by the companies themselves, to have a code of conduct?

Edward Lucas: First, I think we need to have a code of conduct. They cannot say, "This is our black box. There is nothing to discuss." Just as we expect food companies to be able to tell us what is in the food—we have all sorts of standards about safety in all sorts of businesses—there is no reason why the information and communication service providers should be able to say, "Sorry, black box, nothing to see here."

The key thing is that they should give us better clues about what we are going to see. My evidence to the Committee—I have got one of the slides, which I hope you can see—shows what Google already does. If you are searching a site on Google, it quite often will put up a thing saying, "This site may be hacked." It does not stop you from clicking on it, but your Google search results on any computer—any browser—will just give you a bit of a warning that there may be something funny here, possibly because they collect huge amounts of data.

They could also do a thing saying, "This site may not be real". For those of you who are more technically minded, the whois search is very revealing. If you go to Bill Browder's website and do a whois, it shows that it is him; there is a phone number, an address—it's all there. My former employer *The Economist* gives that—we want people to know who we are. Go to some of these dodgy sites I mentioned and the whois registration, which is like your internet birth certificate, has been intentionally obfuscated. That means that someone went to the corner shop, bought a prepaid debit card

for £100, went to an internet café, bought the domain name—just as I bought your domain name—bought some space on a computer, launched the website and completely concealed what they did. I think the search engines should give us a warning that this may not be real.

Secondly—going down the slide a little bit, to this red screen here—if you go to a dodgy site on the Chrome browser, for example, Google gives you a very helpful red screen. This one says, "Deceptive site ahead. Attackers on" this site "may trick you into doing something dangerous like installing software or revealing your personal information". That is a very useful public health warning. There is another one which just says that a site may have malware on it which may harm your computer. We're therefore already used to the idea that you get these warnings.

They don't say, "Don't do it". Interestingly, you used to have to say, "Yes, I know what I'm doing". They found that most men, confronted with a button saying, "Yes, I know what I'm doing," clicked yes on principle. I know the guy at Google who is responsible for designing these things. He did a lot of testing of the shade of colour, the typography and the phrasing, so they got it down to a very low level of people clicking through.

I think we should be saying something to these three platforms—almost every link we click on comes from Google, Twitter or Facebook. Very few people type, for example, "dcmscommittee.parliament.uk" into a browser—you do it by searching. You should get a warning when you are searching if there is something that is not on there—if there is no street address, no phone number, no real people, no whois registration—and then you would know. You can still go there. It may be a wonderful parody account that exists about you, or the world's best jokesmith making fun of Mr Browder or me or your Committee or whatever, and that is fine—I'm not against it—but at least you should know that this is not a real thing and that when you have got to the real thing it really is the real thing.

Q881 **Brendan O'Hara:** Mr Lucas, let me just follow up on something you said to my colleague Mr Watling. You said, "Don't look in the mirror; look in the windscreen at what is coming down the road." What is coming down the road, and how does that compare with what we have already experienced from Russia?

Edward Lucas: It's going to be a lot worse. Bill has already touched on this. The so-called "deepfakes"—the audio and video that look and sound like a real person saying something that that person has never said—use software that is already available now. Pornography is always the driving force on the internet, and you can create a pornographic movie with any face you want superimposed on the actors in the porn movie. There is a very good example of Barack Obama delivering a speech by George Bush. It is all a little bit clunky and works better in black and white than in colour—slightly grainy, clunky video is more convincing in a way, because it looks like something that people might have shot on their phone. So we are rapidly moving into an era where the Russians or any other adversary

can create our public figures saying or doing things that are disgraceful or highly corrosive of public trust. And we are not remotely ready for this.

What would your constituents think if they saw a video of you on YouTube saying, "I've been thinking about this? I think Scottish independence is a really bad idea"? But that could happen next week. Or it could be Mr Collins saying, "You know what, I'm going to join the SNP." We could do this. This is going beyond the era of cartoons—it is the sort of stuff you have previously only seen in cartoons, but now it is going to be happening in audio and video that, for most people, will look completely convincing. And that offers huge scope for our attackers; you could have a commander-in-chief of an army telling his soldiers to surrender.

Q882 **Brendan O'Hara:** How far away are we from that?

Edward Lucas: I could play you something—though my screen is rather small. My former paper, *The Economist*, wrote a cover story about this a few months ago, and the technology has already moved on since then. If you just Google "Obama Bush", or "deepfakes", you will see examples of what can be done already.

Q883 **Brendan O'Hara:** Is Russia the only main state actor indulging in these activities?

Edward Lucas: I think Russia is particularly engaged. We notice what Russia does particularly, because Russia is close to us and a threat, but if we are talking more broadly about influence operations, I would say the Chinese—what the Chinese are doing in Australia is extremely worrying. I think there is a sort of malevolent ecosystem where the Russians, the Chinese and possibly others are learning from each other about how to conduct these operations.

Q884 **Brendan O'Hara:** What are the Chinese doing in Australia?

Edward Lucas: For example, they are trying to close down debate on China in Australia by leaning on the Chinese diaspora—look at *The New York Times* a week ago—and it has become increasingly hard. The Taiwanese are basically being discriminated against in Australia through the exertion of Chinese state power. The Tibet cause has been suffering cyber-attacks, harassment and intrusion. The Australians have actually introduced a new counter-subversion law that makes it a criminal offence to interfere with an Australian's democratic right or duty. In fact, the author of that law, the former Attorney General, is going to be coming to London as the new high commissioner here quite shortly, so you will be able to discuss it with him. I only know what I have read in the papers, but it seems to me that there are a lot of interesting echoes, parallels and possibly pre-earthquake tremors in the Australian thing.

Q885 **Brendan O'Hara:** I presume that fake news and the spread of disinformation is just one of the many weapons in Russia's armoury. How does that fit with its overall strategy? I suppose the question would be, what is its endgame?

Edward Lucas: Bill knows a great deal on this as well. There is a huge discussion about whether Russia is basically just a kleptocracy and all this other stuff is just designed to disguise the huge stealing machine; whether it is a kind of Soviet Union redux that wants to restore a geopolitical buffer zone around Russia and to make neighbours do what they are told; or whether it is an attempt to divide and rule the West so that the West cannot constrain Russia with rules that Russia does not think are fair. I think all those explanations have some weight to them, but I rather defer to Bill. What is Putin's endgame?

Bill Browder: In very simple terms, while the rest of the world's economies have been growing—China, Europe and the United States—Russia's economy has been stagnant, because it is a totally dysfunctional place, so Putin cannot bring Russia up to the level of the rest of the world. So, in broad terms, what is all this about? It is his objective to bring the rest of the world down to him.

How does he do that? First, he wants to get rid of all opposition to him, and the opposition comes in the form of a large United States, which is a big country, so to the extent that he can create chaos in the United States, people aren't paying attention to him. He doesn't like the European Union—he can pick off individual countries, but he cannot pick off a large bloc like the European Union, so his objective would be to create the dissolution of the European Union. He doesn't like NATO, because NATO, again, is a large bloc of people who could stand against him, so he would like to find ways of destroying the confidence that NATO members have in one another.

How does he do that? We are focusing on a subset of these issues, which is social media and fake news, but just a couple of days ago Putin used gas as a weapon, with the Russians cutting off gas to Ukraine for the umpteenth time. They use financial weapons all over the place. One of the main objectives in my campaign is to track down the laundered money that led to the murder of Sergei Magnitsky. We have discovered that Russia has corrupted different officials in different countries. For example, Switzerland had a major money laundering investigation that was initiated by this Alexander Perepilichnyy, the one who died here, and we discovered that a senior federal police officer in the Swiss police was a mole for the Russian Government—he was paid by the Russian Government. He has been fired, and there is a criminal investigation going on. We have discovered that there is a woman in the prosecutor's office in Cyprus who is effectively under the undue influence of Russia.

The Russians are out there poking away in all different ways—with fake news, with abusing international legal treaties like Interpol, with gas, with money—and their objective, very broadly, is to bring the rest of the world down to them. And they are doing a pretty good job so far. It looks like we are all at war with each other, and no one is paying any attention to Russia.

Q886 **Brendan O'Hara:** Causing chaos doesn't really seem like a strategy? Is it a strategy? Is it a thought-out strategy?

Bill Browder: It is not a strategy; it is a tactic.

Q887 **Brendan O'Hara:** So what is the strategy then?

Bill Browder: Well, you should say, what is the objective? Vladimir Putin's objective is to stay in power and to keep all his money. How does he stay in power and keep all his money? It's not easy with a bunch of people in his country who are—I mean, any person, whether you are the best leader or the worst leader, if you have been around for 17 years, people start getting tired of you. And in his particular case, they're getting tired of him, and the economy is not doing well, and people are getting poorer. So what do you do? You go out and you start wars, you create chaos and you create foreign enemies. This is all sort of "Machiavelli Dictator's Playbook 101" that Putin is after.

So what is his strategy? His strategy is to have foreign enemies that are not at war with him. He can't be at war; he's got to have an asymmetric war. He could not survive a real military conflict. This is a perfect asymmetric war: to pretend you're not doing it, to send in little green men to Crimea and then say, "No, they weren't ours", and to do all this stuff where you spend $1.5 million a month sending out messages from the internet research institute in St Petersburg, and things that are plausibly deniable, which have a huge effect, but do not require huge resources to do. He's become the expert at asymmetric war.

And we are at war with Russia—there's no question. With our democracies and our slow reactions, he's able to do this stuff because he doesn't have any democracy or any oversight. He can wake up one morning and just decide he's going to do something. He doesn't have to go to Parliament; he doesn't have to worry about the courts; he doesn't have to worry about the electorate, because the electorate is fully—everything is fully—controlled. So, he can sort of dance around and do all these tactical things.

I would say he's not a strategist. This strategy is not going to work for him. In the end, we're all going to anger to such an extent that we will come up with solutions for all the stuff he's doing. Democracies are slow to anger, but when we do it's going to be devastating for him. But it's going to take a while, and it's good that there are Committees like this that are looking at the issue, because eventually these Committees will come up with recommendations that will stop him. It's slow, it's frustrating and it's a bit demoralising while it's happening, but I'm convinced that he's not ultimately a long-term—his long-term strategy is not ultimately going to succeed, because we actually have a lot of power and once we figure out how to use it—

Q888 **Brendan O'Hara:** So what are the UK Government currently doing to tackle this issue? How does what the UK Government are doing compare with other countries, and is there evidence of best practice that either of you can point to, which you would advise the UK Government to use?

Edward Lucas: I think the UK Government made Russia a tier 1 national security threat, and it's developed a strategy. Some elements of that strategy have come out. We have the beginnings of a whole-of-

Government approach, but it's extremely difficult. When you try a whole-of-Government approach on Russia, everybody's treading on everybody else's toes, and what we have seen so far in Whitehall is that there's been a massive turf war, rather than anything that's actually dealing seriously with Russia.

We need to protect ourselves better; that's one element of it. We need to try and constrain Russia—make Russia pay a price for doing things we don't like. We need to try to engage with Russia on some things and deliver very tough messages to them. We need to build up our resilience, and we need to try and find the next generation of people in Russia who may be in charge and see if we can talk to them.

However, I think the key thing we've got to do, and this is something that's very close to both Bill's heart and mine, is that we've got to understand that we can't put prosperity ahead of security any more. If we think that only money matters, then we're defenceless when people attack us using money. For 20-something years we've treated Russia just as an emerging economy, and these things as some political bumps in the road, thinking that nothing should get in the way of trade and investment. And the result is that dirty Russian money has flooded into the City; it's flooded into the London real estate market, and it's flooded into all sorts of other places.

That has created lobbies in this country who are extremely unhappy at the thought of relations with Russia going downhill, and you get those lobbies exercising power in all the political parties. So we've made it much more difficult for ourselves to constrain Putin on what is fundamentally his biggest weakness—$800 billion, which the Americans reckon is the amount of state-related Russian assets abroad, with $300 billion of them in America and the rest elsewhere.

As Bill has been so admirably campaigning for, we should be freezing and seizing and using that as a way of exerting pressure on Russia. But we don't, because as soon as you try that you get very rich, influential people in our system coming along and saying, "Hang on a moment, that's my business. I sell luxury flats to Russians. Don't get in my way." Unfortunately these big City law firms—big American law firms—are playing this scandalous role of laundering Russian money behind attorney-client privilege. We have a great deal of house cleaning to do, I'm afraid.

Q889 **Brendan O'Hara:** Is there best practice that you can point to? Is someone getting it right?

Edward Lucas: I think that the Nordic, frontline states have very good threat awareness. I think we have a lot to learn from Estonia, Latvia and Lithuania on some things. Sweden and Finland are very good. The countries that have been warning us for longest are the ones we should listen to. One of the things that most annoys me is when people treat this as a new problem. It is not new. It is new to people who have not been paying attention. We were warned even back in the 1990s about this, and we ignored and patronised the people who were giving us the warnings.

Q890 **Paul Farrelly:** I am one of 11 Members, with a majority of 30, of what I call the "Under 100 Club" in the House of Commons. A few hundred votes can change a Government. You rightly mentioned that the general consensus is that Russia is out to destabilise and sow doubt. The opinion has been put to us in some of our discussions that actually the Russians are a sideshow when it comes to influencing elections. It is really private companies as paid agents that we should be more worried about, particularly as targeting techniques get more sophisticated. Therefore the question is what to do if you decide that it is right to regulate that, as political advertising is regulated in other spheres, such as public service broadcasting. What is your opinion on that?

Edward Lucas: As I said before, advertising should be transparent. We need to know if someone in your constituency is buying advertisements targeting your voters. We all have the right to know that. It is no good Facebook just saying, "Sorry: black box. Can't help you." It is potentially illegal. If there is money going into that, it should be going on someone's elections expenses. These rules vary by country, but in our country, we are very strict on what can be spent in an election and we should enforce those rules. We need an open register of advertisements, certainly for political speech—I would argue, for everything. We need data about realness. Mr Farrelly, I have forgotten what your constituency is.

Paul Farrelly: Newcastle-under-Lyme.

Edward Lucas: So if someone sets up "Newcastle-under-Lyme concerned citizen" on Twitter and is Tweeting away saying, "Mr Farrelly is a very idle MP and never turns up," you should be able to know—we all should be able to know—does that person actually exist? How much realness is there? Suppose that there are 1,000 Twitter accounts and Facebook pages, we need to know who is behind them and how real this is. Once we know that, we can start applying the same criteria. There are people who shout outside Parliament everyday about various causes close to their hearts, and they are quite smelly, and you can tell quite a lot about people if they are smelly and dressed strangely, and we know that that is not the same as a real demonstration with real people. Evolution has given us senses to make these distinctions. On the internet, all we have is what is on that 2-D screen, so we need more help in knowing whether we are to take seriously this thing that we see on our screen.

Q891 **Giles Watling:** I want to ask a direct question that Mr Farrelly touched on. He said that a few votes can change everything. In your opinion, is Russia just a sideshow on this, or is it commercial things we have to concern ourselves with?

Edward Lucas: I think the vulnerabilities should concern us. Russia is exploiting these vulnerabilities because they are there. If Russia was not exploiting them, other people could. If the vulnerabilities were not there, Russia would be looking for other vulnerabilities to exploit. So I think there is a kind of matrix. You have a list vulnerabilities and a list of threat actors, and at this point Russia and the vulnerability coincide.

Bill Browder: I don't think Russia is a sideshow at all. When you talk about Russia and then you talk about private businesses, Russia almost never does it in the name of the Russian Government when they get involved in activities. Everything is done by a proxy and it is all done very informally, where the Government allow some business person to become wealthy in some area, and then a phone call is made and that business person then does something that the Government want them to do. That has become a big problem in America. There is a piece of legislation called the Foreign Agents Registration Act, which is a way of creating some transparency on whether a foreigner is trying to influence US policy. For countries like Russia, their Government isn't trying to dictate policy; it will be some private person. Where is that line getting drawn?

It comes back to what Ed was saying. If you have transparency and disclosure about who is doing what in political manoeuvring—whether it be advertising or lobbyists or whatever—if there is some disclosure, it is much easier then to say, "Of course they would say that; they are the Russians," or, "They're a business representing the Russians," than if we just don't know who is saying what and then someone sounding very credible shows up, or some advertisement or article keeps on popping up, that makes people believe something and you don't know where it comes from.

Q892 **Chair:** May I ask in closing whether you think there needs to be a more co-ordinated approach across government to deal with the Russian threat, involving different Departments working together?

Edward Lucas: Not just across government but across Governments. I am afraid that these big communications service providers are not scared of individual Governments, but they might be scared of Governments acting together.

I know views on the Committee will differ on Brexit, but the European Commission did quite a good job of bringing Microsoft to heel over its monopoly thing. We have ways of making these companies come to heel and taking very big commercial hits, whether we do it at a G20 level or G7 or OECD level. I do not think any one country will be able to do all this on its own.

Russia is attacking us with, I reckon, 20 different tactics, which affect almost every bit of government, from universities to the criminal justice system to our intelligence agencies and our financial system. We are not pulling those things together. I am now pushing as hard as I can, both within the Committee system and within Whitehall, to get over these turf wars and to start actually treating Russia rather as we treat terrorism.

When we look at terrorism, we don't say, "That's terrorist financing; that's money, so we don't do that." We look at the whole thing, from propaganda to money to the way they acquire their weapons; every single bit of it. We need the same approach for Russia.

Q893 **Chair:** Finally, you mentioned Committees. If Government Departments won't work together, do you think there should be a special Committee of

the House that investigates the Russian threat?

Edward Lucas: I think the ISC would be a good place to start, but it is very important that, when the ISC looks at this, they don't simply ask the agencies what they are doing. They should be talking to the Bank of England and the Financial Conduct Authority, and they should be taking evidence from people like Bill.

There is a large amount of expertise in this country that is now outside government because we have systematically eviscerated our Russia-watching capability over the last 25 years of complacency and arrogance. We need to hoover up all the capability we have, and also look at the entire breadth of the Russian threat.

Q894 **Chair:** Do you have any final words, Mr Browder?

Bill Browder: I think that, in order to solve the problem, one needs to recognise the problem. I like your question, which is that this is a subset of a number of other things that the Russian Government are doing. They are absolutely doing it with great vigour. It is well resourced, and they will continue to do it until we come up with ways of stopping it.

To the extent that you can act on fake news and social media, that is great. To the extent that you can feed this in or create a more robust parliamentary response on Russia, which creates a more robust Government response, that would be a fine outcome—and an eventual outcome, one way or another. It is a problem that we will all have to deal with.

Chair: I thank you both for your evidence this morning. It has been extremely interesting. I thank you, Mr Browder, for the work you do here and around the world and the personal risk you take in speaking out on these issues.

Examination of witness

Witness: Elizabeth Denham.

Q895 **Chair:** Elizabeth Denham, thank you very much for joining us today. I know that some Members are coming back, but we might start straightaway, if that is all right, as we are running a little late.

Can you start off by giving the Committee an update on your inquiry into the use of data analytics for political purposes during the UK's referendum, the scope of that inquiry and perhaps when you expect to report on it?

Elizabeth Denham: We launched an own-motion investigation in May 2017, because we were concerned—and I think the public were concerned—with reports about the use of data analytics, the micro-targeting of voters and various partnerships between commercial campaign and political parties being able to use personal information in ways that people might not understand.

Our investigation is comprehensive. It is a high priority for my office. I have about 10 people working on the investigation full time. It involves more than 30 organisations—social media platforms, as well as data analytics companies like Cambridge Analytica—and political campaigns and parties.

What we are trying to do in this investigation really falls along two tracks. On the first track, our intention is to be able to pull back the curtain and explain and expose for the public, parliamentarians and civil society what happens with their personal information in the context of political advertising and political messaging. The second track of our investigation is, if we find contraventions of the Data Protection Act, we will be taking enforcement action. That enforcement action could take some time.

So, parallel tracks. On the first track, we intend to publish a report that really does expose how personal data is being used in this context. We expect that report to be published in the spring. In terms of enforcement activities against contraventions of the Act, that will take as much time as I need, to ensure that I have crossed all the t's, dotted all the i's and followed the legal processes, and due process and fairness for the organisations involved.

Q896 **Chair:** Are companies like Facebook co-operating with the inquiry to the extent that they are letting you see how they hold data and use it? We are told repeatedly that it is a closed system and they do not allow people to look at how they manage data.

Elizabeth Denham: Facebook has committed to co-operate with our investigation; Twitter and Google as well. We have served seven information notices—that is the legal tool I can use—to ensure that we are getting a formal, comprehensive answer to the questions that we have asked. Of the seven, one is before the tribunal and the rest have not been challenged. I expect that we will get the information that we need. I will be serving about five more notices this week.

Q897 **Chair:** Perhaps you can explain a bit more about that process. You have not been able just to ask them for the information; you are having to serve a notice and go to tribunal in order to obtain it.

Elizabeth Denham: I can simply ask for information, but I prefer to use the information notice provision because that is a formal process and it is very clear to the organisation what information we are seeking. It also gives them the ability to challenge my information notice before the tribunal if they do not agree that they should share that information. So far, we have had co-operation from most of the organisations. We hope that we will have all the information that we need to be able to finish our investigation.

Q898 **Chair:** How can you check that you get all the information you asked for from the companies?

Elizabeth Denham: In an information notice, if we ask the question, they are legally required to give a fulsome answer. If not—if we find

information that has been left out down the road—we have the ability to enforce that notice through a civil monetary penalty.

Q899 **Chair:** But with a company like Facebook, how would anyone check or know?

Elizabeth Denham: We have asked the social media companies for a complete description of the ecosystem in which their advertising works. For the public, we need to be able to understand why an individual sees a certain ad. Why does an individual see a message in their newsfeed that somebody else does not see? We are really the data cops here. We are doing a data audit to be able to understand and to pull back the curtain on the advertising model around political campaigning and elections.

Q900 **Chair:** The reason I am asking is because one of the interesting things for our inquiry is about the powers you have and whether they are sufficient. To use your analogy, it sounds like you are not peering behind the curtain. You are asking the person behind the curtain to pass information back to you, but you cannot actually see what they are doing.

Elizabeth Denham: I can also see what they are doing. We have other tools. We can serve a demand for access, which is like a warrant with notice, so we can go in and look at the computer systems. We can seize computers and take images of the computers. That is more than just asking for explanations. We have the power to file a demand for access and, if need be, I will do that because we really need to get to the bottom of how data flows, how analytics work and how algorithms are determining the messages that are disseminated and received by individuals.

Q901 **Chair:** What grounds would you need to make a request like that?

Elizabeth Denham: For a demand for access?

Chair: Yes.

Elizabeth Denham: Or even a warrant—we have warrant powers as well—we would have to go to the judge. A warrant has a surprise element to it, so a demand for access is my preferred method. That would be if we were not receiving co-operation or if we needed to ensure that we preserved the evidence for our investigation.

You also asked whether I think I have the powers that I need to carry out what is becoming an increasingly difficult area of responsibility—the Information Commissioner's Office. In my parliamentary briefing on the Data Protection Bill, one of the deficiencies I see in terms of my powers is the ability to enforce an information notice. In the Data Protection Bill, I suggest to Parliament that I do not want a fine to be the result of an organisation refusing to co-operate with us. I actually want the information in an inquisitorial investigation. People should not be able to buy themselves out of compliance with our office's investigation. I have had good conversations with Government about my need to be able to enforce a notice, to receive or to preserve information, rather than just fine a company at the end of the day for not co-operating.

Chair: That is very helpful. We have a session with the Secretary of State next week, and I am sure that is something we will want to follow up with him on.

Q902 **Ian C. Lucas:** You said that one of the requests for information had been challenged. Can you tell us who by?

Elizabeth Denham: It is in the public domain. It is UKIP that has challenged our information notice, which it has the right to do. Because it is going before the tribunal, that is a public notice. I believe that it will not be heard, though, until May.

Ian C. Lucas: Can I ask you some questions that specifically relate to Facebook? They are also from the perspective of someone who is a politician, who has been involved in political campaigning and who has seen the importance of Facebook in political campaigning increase massively since 2015. That is my perception. I want to clarify something about what it means to share information with Facebook. You are familiar with what a Facebook group is? If someone is a member of a Facebook group, is that information able to be shared by Facebook with any third party, as a matter of current law?

Elizabeth Denham: First, I want to start by agreeing with you that social media is a powerful and important tool in political campaigning. What we want to do and what is really important, through discussions and Committee appearances like this one, is to make sure that social media is used for good, and for increasing participation and bringing people to the table. We want more people to participate in our democratic life and democratic institutions, and social media is an important part of that, but we also do not want social media to be a chill in what needs to be in the commons, what needs to be available for public debate.

We need information that is transparent, otherwise we will push people into little filter bubbles, where they have no idea about what other people are saying and what the other side of the campaign is saying. We want to make sure that social media is used well. It has changed dramatically since 2008. The Obama campaign was the first time that there was a lot of use of data analytics and social media in campaigning. It is a good thing, but it needs to be made more transparent, and we need to control and regulate how political campaigning is happening on social media, and the platforms need to do more.

You are asking me a precise question about Facebook groups and whether Facebook can share information that is gathered in a group. The answer, unfortunately, is that it depends. When you say "with third parties", it depends whether that is with third party advertisers, for example, third parties outside or third parties in the Facebook group of companies. The reason that question is such a good one is that it goes to the heart of what the first part of our investigation will do, which is to explain how data is shared on Facebook. Rather than give you a specific answer on the Facebook group, I will point you to our report, which will explain how information is shared. It is still a bit of a black box. Facebook is mixed.

Q903 **Ian C. Lucas:** So it is coming—?

Elizabeth Denham: In the spring.

Q904 **Ian C. Lucas:** So I need to wait to see it. Can I ask you another question? Can I present you with a picture, which is me as a candidate, wanting to reach as many of my constituents as I can to deliver my political message? Can I go to Facebook and say to them, "Will you sell me advertising to present my political message to as many people as possible, who I want to influence to vote, who have particular characteristics?" Is that legal?

Elizabeth Denham: It is legal if it is transparent and Facebook is not sharing information with you, but you are going to Facebook and saying, "I want to reach people who look like this. I want to direct this to my constituents. I want to direct this message." You are directing Facebook to be able to deliver that message. What I am going to suggest is that there needs to be transparency for the people who are receiving that message, so they can understand how their data was matched up and used to be the audience for the receipt of that message. That is where people are asking for more transparency.

Q905 **Ian C. Lucas:** What I also think is important, because I did not know this until I started this inquiry, is that being a member of a Facebook group means that I am consenting to Facebook doing that.

Elizabeth Denham: In the terms and conditions in the fine print, there would be the ability for you to understand that, but we want Facebook to do more. We want social media companies to do more on transparency. At this point, I think nobody is making the argument anymore that these are benign platforms. They have informational fiduciary responsibility to make it clear to people how their data is used and shared to be the recipient of a certain kind of message or to be profiled in a certain way. That is the kind of exposé that will be in my report, but I am happy to speak to you offline as well if that is helpful.

Ian C. Lucas: Thank you very much, that is very helpful.

Q906 **Giles Watling:** You said somewhere in the paperwork that you fined TalkTalk, I believe, some £400,000 for not protecting data from cyber-attack. Touching on what Damian said earlier, for a company like TalkTalk that is neither here nor there, I would imagine—that's back-pocket money. So it is not enough. What would give you more teeth? What would you ask for to give you more power, more teeth, to really deal with something? Not protecting people's personal data from cyber-attack, if you are a big company like TalkTalk, that's really important, but you are just slapping it on the wrist.

Elizabeth Denham: The good news is that although the general data protection regulation is only just on the statute book, it comes into effect on 25 May 2018. Under the GDPR and with the new Data Protection Bill, I will have many more tools in my toolkit, including more significant sanctions and fines—up to 4% of global turnover, or £17 million, whichever is greater. I think that is a very useful set of sanctions and

powers to be able to use against big companies. Because I agree with you, £500,000 is not significant for really big players.

Q907 **Giles Watling:** Do you think that will be enough for you? Will that do it?

Elizabeth Denham: I think what is even more powerful is the ability to order a company to stop processing data, or to delete data, because that will hit a company in its services. If I found a contravention of the Data Protection Act or of the GDPR when it is in force in a few months, and I ordered a company to stop processing in a certain way or a certain type of personal data, that would hit its bottom line, as well as the reputational damage.

Also, we will have the ability to do compulsory audits so, back to the Chair's question, if I suspected that there was a contravention, I would be able to do a full audit, including of information technology systems. Right now I do not have the ability to do a compulsory audit, and that audit is a very powerful tool.

I think that we are about to get more significant powers that will help us. It will be really important that companies and organisations comply with our visits and investigations, otherwise we will be going to go to court in extended litigation, which I would like to avoid.

Q908 **Chair:** We may only have a bit longer. Would it be possible for us to receive a copy of your recommendations to Government on how the Data Protection Bill should be amended to give you the additional power to get access to the data, not just to fine companies?

Elizabeth Denham: Yes, I will write to you, but it is also in my parliamentary briefing on the Bill. That is published and there is an extensive note about my information notice powers.

Chair: That's great.

Q909 **Giles Watling:** I just had a follow-up. The way that data are collected is a hidden way—you were saying behind the curtain. How do you ensure that people's personal data are not being illegally used?

Elizabeth Denham: We have an intelligence unit that is looking at systemic issues that are reported either in the media or by individuals. But I agree with you that the traditional complaint mechanism where a regulator like us would sit back and wait for someone to complain does not work any more, because there is so much data processing that is opaque and in order for us to be able to act effectively, we have to look at the horizon, we have to understand how companies are processing data, and we have to step in and do some of these own-motion investigations, like the one that I am doing right now. I have put a lot of staff and resources into this, because I think it is really important. We didn't wait for a complaint about social media companies, micro-targeting or hyper-personalisation of political messages. We knew that these were the issues and therefore we can act. So now we will be able to do audits, comprehensive investigations, reports to Parliament and public reports, and we will be able to take enforcement action and sanctions.

Data protection is not a back-room, back-office issue anymore. It is right at the centre of these debates about our democracy, the impact of social media on our lives and the need for these companies to step up and take their responsibilities seriously.

Giles Watling: Thank you.

Q910 **Simon Hart:** I just want to go back, if you will forgive me, to the question about Facebook advertising because there was one area I was not completely clear about. Facebook have made, could we say, a play to MPs, and presumably to Assembly Members and others, about the effectiveness of this. I have had conversations in which they have said, "We can demonstrate to you that in your constituency there are x thousand people who have an interest in certain subjects"—and politics might be included in that list of subjects they have identified as relevant to that person—"So in Carmarthen West and South Pembrokeshire there are 4,850 people who have mentioned politics and who you can therefore specifically target with advertising that we will offer you at x pence per like." I have to say that that sounded like a pretty tempting offer—miles cheaper than any other form of micro-targeted advertising you might engage in. But it never crossed my mind until during the question you were just dealing with to consider how they acquire that information and whether the 4,800 people who have mentioned politics knew that Facebook would use that to facilitate me or Ian Lucas to target them. Do they know that? Do those 4,800 people know that that is the use to which Facebook will commercially put their data?

Elizabeth Denham: I suspect they do not. We have run some focus groups to be able to understand what people do or do not understand about the compilation of their data and the world of big-data politics. That is a really important part of our report. A recommendation I am considering right now, coming out of this report, is that I think the use of social media in political campaigns, referendums, elections and so on may have got ahead of where the law is. I think it might be time for a code of conduct so that everybody is on a level playing field and knows what the rules are. I think there are some politicians, some MPs, who are concerned about the use of these new tools, particularly when there are analytics and algorithms that are determining how to micro-target someone, when they might not have transparency and the law behind them.

Q911 **Simon Hart:** Ironically, thanks to the GDPR, our ability to use our traditional databases of email addresses that we have carefully and legally harvested over the years is potentially going to be compromised in two months' time. So there is going to be a greater reliance, because we would argue that the opt-in process is probably going to result in an awful lot of people who are just historically on databases disappearing. So there is going to be a greater focus and a greater reliance on using micro-targeted social media advertising than has ever been the case in previous elections. Would it be fair to say that there is some urgency in getting these codes in place? Whatever the next big election is in the UK, or whenever it is—who knows—undoubtedly I suspect that I, for one, am going to rely much more heavily on that than I ever have done in the

past.

Elizabeth Denham: In our conversations with political parties I think there is agreement that there need to be clear rules of the road when it comes to using social media and data analytics to target individual voters. But if there is an agreement on, "let's get it right", it goes to trust, transparency and integrity of the democratic system.

Q912 **Simon Hart:** This is my last question: did you happen to see the evidence session with Cambridge Analytica last week?

Elizabeth Denham: I did.

Q913 **Simon Hart:** Were you reassured or panicked by that?

Elizabeth Denham: I know that the Committee understands that I am constrained because we have an active investigation under way and I would not want to prejudice my investigation. But yes, we are looking at Cambridge Analytica.

Q914 **Brendan O'Hara:** I have a couple of questions on the Data Protection Bill, which had its Second Reading last night. Other than the issues you highlighted, are you generally satisfied with the provisions contained in the Bill?

Elizabeth Denham: I'm generally satisfied with the Data Protection Bill and I think there is urgency in passing the legislation and ensuring that we are bringing the GDPR into force, as well as the law enforcement directive and the rules for national intelligence agencies. There are some issues that I have brought forward for Parliament and that is in the parliamentary briefing. I talked about information notices. I still have some ongoing concerns about the Government's framework for data sharing, where the Secretary of State makes some rules. I worry about conflict and confusion with my own codes of practice for data sharing.

Q915 **Brendan O'Hara:** Are you satisfied that the Government's interpretation of our derogations will make us compliant with GDPR? Or do you have concerns about the derogations?

Elizabeth Denham: I don't have concerns about the derogations in terms of us being able to meet the standards of the GDPR and potential alignment with Europe on exit. I don't have concerns there.

Q916 **Brendan O'Hara:** What about the derogation against the backdrop of achieving adequacy? Is that something that you have considered and could that be problematic?

Elizabeth Denham: I don't see anything in the derogations in the Data Protection Bill that would compromise an adequacy assessment. I don't see anything directly in the derogations. We have to remember that, if there is going to be an adequacy assessment, it will be done in the round and it will be done comprehensively by the European Commission, where the Commission will be looking at our intelligence gathering, the bulk collection of data and whether there is proper oversight and transparency for the collection of data by the intelligence agencies. That is one thing.

They will look at our laws in the round, and I don't have specific issues about the derogations—

Q917 **Brendan O'Hara:** So you have no concerns, when the Data Protection Bill is finally passed, that the form in which it is passed could compromise an adequacy agreement?

Elizabeth Denham: Not the derogations—

Q918 **Brendan O'Hara:** But the Bill.

Elizabeth Denham: The Bill itself. I think there is even strengthening of some of our powers on oversight in the Data Protection Bill. I think the amendment for our office to do a code of practice for the architecture of children's apps and websites is a really good addition.

Q919 **Brendan O'Hara:** So you've no concerns about adequacy?

Elizabeth Denham: I have no concerns about the derogations and the impact on adequacy.

Q920 **Brendan O'Hara:** But have you no concerns about achieving adequacy?

Elizabeth Denham: I think if the Government decide to go down that route to get an assessment of adequacy, that is the right way to go. There will be some challenges, especially related to our national security agencies and bulk collection and retention of data.

Brendan O'Hara: Thank you.

Q921 **Paul Farrelly:** Can I congratulate you on this proactive inquiry? It is certainly very timely. We started off here with a blank sheet of paper, and that blank sheet just keeps getting bigger and bigger. Your evidence today has raised issues in my mind about consent at all sorts of levels. I don't know myself what consent I have given Facebook by virtue of using it and having an account. If I don't know, I am sure that my now 19-year-old son, to the extent that he is still on there with us old fogies, knows what he gave when he gave a false birthdate that he since cannot alter.

In terms of your answer on the issue of politicians possibly having a code of practice, you have also flagged up another area that we haven't looked at. If you have a submission to make on your ideas about a code of practice, that would be useful. Chair, I think we should also ask the Advertising Standards Authority to make a submission on the regulation of political advertising, because at the moment we can get away with anything as long as it is not libellous and therefore the billboards or the newspapers won't run it, because we are exempt.

Can I ask one question that might inform us further? Are there any similar inquiries to yours going on in the European Union by agencies equivalent to yourselves?

Elizabeth Denham: Not that I am aware of. I think this is a really important inquiry. I know that my colleagues across Europe are watching it very carefully, and colleagues in Canada and Australia as well. I think that taking a comprehensive approach and looking at the data brokers, the data analytic companies and the social media platforms, as well as campaigns and parties, is the way to go, so that people can understand how the data is flowing and where some red lines may be.

Q922 **Paul Farrelly:** So this is truly groundbreaking, really? I would find it difficult for us to publish a report without the benefits of your reports and your findings, and you actually explaining to people like me how things work.

Can I just push you on timing a little bit more, because spring, by various definitions of when seasons start and finish, could go up to the longest day—21 June?

Elizabeth Denham: I'm hoping that it will be before the end of May. Again, we need some more pieces of evidence and some more detail, but I really decided that this twin-track approach is the way to be able to give some policy advice to your inquiry and to agencies in the UK, while continuing down the road of enforcement action, which takes more time. That's why I think that dividing it in two might make more sense. Being able to explore the advertising ecosystem of social media platforms and how it works in political campaigning will be, I think, of huge value to inquiries like this one—I hope.

Q923 **Paul Farrelly:** I'm sure we will want to liaise with you further, when we see the lie of the land on the timing of our report.

I've been on this Committee since 2005 and the first time the Information Commissioner's Office really came to the fore was in another invaluable, proactive investigation that your predecessor—Christopher Graham—undertook, which was Operation Motorman. That was widely commended and was invaluable for our reports into press standards, privacy and libel at the time. It was good as far as it went, and it wasn't simply a question of powers for the Information Commissioner's Office; it was a question of resources.

In that case, Steve Whittamore and a number of other individuals were prosecuted, but no journalists or publications, which commissioned illegal acts, were taken on. The view was that the office simply didn't have the resources to take on batteries of QCs employed by powerful and rich media organisations. How does your office stand—potentially—in terms of resources if these much bigger corporations wish to stand in your way and fight you?

Elizabeth Denham: You may have seen that recently we have prosecuted a number of private detectives, but as well as prosecuting the private detectives for their data protection contraventions we have prosecuted their clients—the people who directed their activities. We have done that quite recently. But you are asking me about whether or not I have the resources to be able to take on what might be a very litigious

environment, because we have higher sanctions, so there is more at risk for organisations.

We have recently been given pay flexibility by the Government to be able to retain our expert staff and recruit more expert staff. We need forensic investigators, we need senior counsel and lawyers, we need access to the best, and maybe outside counsel, to be able to help us with some of these really big files.

So we do have the ability. We also have a new fee regime. The ICO is mainly funded by data controllers, so there is a new fee regime that is coming into place. We are relatively confident that we are going to have the funding to be able to do this. It's courage, and it's money, and it's expertise.

The courage comes from being able to pick the right files—the right investigations—that have an impact on organisations and what citizens care about. We have to do that. We also have to have the funding to be able to pay and retain our staff and get expertise when we need it. We need to get on with it. I think that the ICO has shown in recent months that we are taking on complicated files and complicated issues, and have the courage to do that.

Q924 **Paul Farrelly:** I'm sorry. I was not aware of all those actions because we have had two general elections, a referendum, and we have Brexit constantly. It would be quite useful to have a list of those actions, if you could let us have one.

Elizabeth Denham: There have been more prosecutions and more administrative monetary penalties issued in the last year than ever before.

Q925 **Paul Farrelly:** A list would be very useful, because this is a live issue. Motorman was seminal in terms of pursuing these activities, as was phone hacking, because they were all interlinked. All the data was used in different ways to harass and to make allegations against individuals in combination; it was not a single issue. It would be unfair to ask you what you think of the cancellation of Leveson 2, because that might have given you more insight into how these individuals and organisations operated, particularly with regard to public officials.

Elizabeth Denham: I think that is a decision for Parliament. I am aware of the conversations and the public discussions around Leveson 2, but on the regulation of the press, in the experience of our office we have not seen any systematic issues with the press of late in terms of their data protection practices. That said, if something were brought to our attention we would act on it.

Q926 **Paul Farrelly:** So it remains a live issue—illegal data blagging for your office.

Elizabeth Denham: We have seen a lot of blagging in many industries. We have seen it with telecom providers, in the insurance industry, and in the automobile rental industry. We are chasing these—

Q927 **Paul Farrelly:** The legal industry, as well.

Elizabeth Denham: We have seen it, and we have prosecuted. If it is helpful to the Committee I will send you a list. We are on the blagging issue, but we are not focused on the press.

Q928 **Paul Farrelly:** Okay. You've got that issue, the live issue, and this is another big issue for you. That then comes back to resources. The investigations have a parallel in that they are proactive and raise questions of resources. You are damned if you do and damned if you don't, because the question that is still hanging over Motorman, which I am familiar with, is: did the ICO do enough? I am glad that you have raised the issue of courage. Are there any other lessons for your current inquiry, from Motorman and previous inquiries, that are at the forefront of your mind, because this is your big one?

Elizabeth Denham: No pressure. It is my first really big one.

Q929 **Paul Farrelly:** It is your big and groundbreaking one.

Elizabeth Denham: Again, I think pulling back the curtain and looking at the policy implications on how to get this right is really important. That said, we will follow enforcement action if we find individuals in organisations have broken the law. In terms of persistency and focus, we have that going on in spades, but we also have to bring in the GDPR—the administration of a whole new data protection regime. There is a lot of pressure on the office right now, but I think we are up for it.

Q930 **Paul Farrelly:** This is the final question, to round this off. Your answer earlier on how you are treating information given to you, and the difference between false information and less than full information, reminded me of the answer given by Ofcom—that there was an assumption that evidence given was not only true, but full, because there were penalties against it. You think, "Hmm." "A lack of curiosity" is a phrase that is bandied around, but how curious are you to follow less than full information?

Elizabeth Denham: Deeply curious. That is also why we are using our information notice power with so many of these organisations, because nothing gets the attention of an organisation more than a formal request compelling the disclosure of information by a regulator, and a comprehensive answer. We have gone back with second information notices when we have not had the fulsome answer. I know that these organisations believe that it is serious and will continue to be persistent and push it, but as I said, it is really important in our new regime that we are able to enforce a notice and not just come up with a sanction like a fine, because really we are after getting to the information at the end of the day.

Paul Farrelly: That could just be a cost of doing business. Thank you, and good luck.

Q931 **Chair:** Let me just close with a few questions. Going back to the level to which you can be satisfied that your information request has been

handled correctly and all the due information has been given, the Committee had several goes at making a request to Facebook for information about Russian activity during the Brexit referendum period. I appreciate that this is a period that you are looking at. We had a letter back from Facebook explaining the methodology that they pursued, how they did it and what they found. We have no way of knowing whether they did that. In a similar situation, do you have to demonstrate reasonable grounds for believing that what you have been told is not true, or can you just challenge it anyway?

Elizabeth Denham: We can challenge it anyway. The demand for access that I was describing earlier allows us to go in and look at systems and records, not just as a set of questions to be answered, but "Show me the evidence of how you carried out this investigation." It is powerful that we have that ability to do it, but this is the first time that our office has used all those tools. It does not mean that an organisation has necessarily done something wrong; it means that they need to take it seriously that the regulator wants a fulsome, comprehensive answer to these questions—"Show me the evidence that this is what you did."

Q932 **Chair:** Yesterday, in the Second Reading debate for the Data Protection Bill, when the Secretary of State was asked about the legitimate grounds for the right to be forgotten, he said that there would be more detail from the Government on that, as well as guidance from your office. Are you able to say a bit more today about what you think the guidance might be in terms of the legitimate grounds for the right to be forgotten?

Elizabeth Denham: The legitimate grounds for the right to be forgotten generally, or are you talking about the right to be forgotten in terms of Google and search engines and the de-linking of information? Are you just thinking generally?

Chair: Both, actually.

Elizabeth Denham: There is a right to be forgotten in our current law. It is mostly applied and used where people come to Google and want de-linking. That is more like the right to obscurity rather than the right to be forgotten. It just means it is really hard to find a report that was inaccurate, out of date and harmed an individual. We get hundreds of these requests to adjudicate where Google has refused to de-link every year, so we are in the business of the right to be forgotten right now. Generally, it is going well. Most of the time we agree that an individual does not have a case for the de-linking of information, because freedom of expression and the right to information has to be weighed against an individual's privacy rights. We are adjudicating that all the time.

The GDPR provides a more explicit and comprehensive right to be forgotten, but it is still a narrow right. If you sign a contract with an organisation—if you are getting public service from a public body—you do not have a right to be forgotten because they need that information in order to provide that service to you. It is really a right that will be reserved for unusual circumstances. We already have some guidance on

our website about the right to be forgotten, and I can certainly send that to the Committee.

Q933 **Chair:** What about the right to be forgotten in terms of data that is held about you if you say, "I want that data back" or, "I don't want my data profile to be used to target me with messaging that I don't want to receive"?

Elizabeth Denham: The right to be forgotten will be used to delete your Facebook profile, for example. Facebook does that now—a legal right to be able to pull all your data, because there is no contractual need for them to continue to process it, but you cannot do the same with your bank because they have fiduciary responsibilities to retain the evidence of how they served you. Do you see that it is a different context?

Chair: Sure. I understand.

Elizabeth Denham: At the end of the day, if a company or an organisation is using a legal basis like legitimate interest to process the data, the right to be forgotten does not apply, but if it is consent in order to continue to process, like Facebook, you have a right to be forgotten.

Q934 **Chair:** What about a more complex case where I have a Facebook account, I have engaged with apps and tools that have been created by developers on Facebook, some of that data may have ended up in the hands of a company like Cambridge Analytica and I then decide I want my data back? Facebook would say, obviously, that you could have the data back from Facebook, because they can destroy it when you leave. They also say that their protocols are that developers and other people who have gathered data from Facebook users should return it, but who is in charge of making sure that happens?

Elizabeth Denham: That is a really complicated question about the ecosystem, where you have this whole chain of companies, especially in behavioural advertising. If you have given your data to Facebook, that is the data controller in that context, but as long as they have passed it on properly and legally, I suspect you are going to have to go to each of those organisations and ask for your data to be deleted. It is going to be a complex system.

Q935 **Chair:** Mr Farrelly just made the point, "How would you know who to go to?" It is not clear who is gathering the data.

Elizabeth Denham: What we are going to conclude in our policy report on all this is that transparency is important. People do not understand the chain of companies involved. If they are using an app that is running off the Facebook site and there are other third parties involved, they do not know how to control their data. Part of the GDPR, which is really important, requires more transparency and control for individuals. The answer to that has to come partially from companies themselves, which have to build this in a way that is accessible to all of us, but it is also the regulator's job to push them towards solutions that work, so that the person is in control and can make choices and decisions about their data and the processing of their data. Right now, I think we all agree that it is

much too difficult and much too opaque. That is what we need to tackle. This Committee needs to tackle it, we need to tackle it at the ICO, and the companies have to get behind us, or they are going to lose the trust of users and the digital economy.

Q936 **Chair:** This has become quite a key area of our inquiry. If people are receiving more disinformation and hyper-partisan content because they have engaged with it in a small way and the data that has been extracted from that engagement is being used to target them with similar material, and they are unaware who it is coming from and why they are receiving it, that has quite severe implications for the way people consume news.

Elizabeth Denham: That is right. All this is about transparency, trust and accountability. Many of your witnesses have spoken about that, and that is certainly going to be the centre point of our report. The GDPR gives more rights to consumers and more responsibilities to companies. It is coming a little late, but there are new powers and new expectations. People need to take up their rights and use them, too.

Q937 **Chair:** Are you able to say anything about your response to the request made by Professor David Carroll for his data?

Elizabeth Denham: Mr Carroll's subject access request is certainly on point for a line of inquiry in our investigation. Again, one of the things we are looking at is how an individual becomes the recipient of a certain message: what information is used to categorise him or her, whether psychographic technologies are used, how the categories are fixed and what kind of data has fed into that decision. We are responding to Mr Carroll's subject access request. He is very interested in the source, or the provenance, of various data that is used to micro-target him. It is a line of inquiry for us, but our investigation is much broader than that.

Q938 **Chair:** Will that line of inquiry form part of the report that you are expecting to publish in May?

Elizabeth Denham: Yes.

Q939 **Chair:** Okay. To what extent do you think it is practical or possible for users to become controllers of their own data, rather than it being controlled by a third party?

Elizabeth Denham: I would like to be an optimist. The point behind the General Data Protection Regulation as a step-up in the law is to try to give back control to individuals so that they have a say in how their data are processed, so that they do not just throw up their hands or put it on the "too difficult" pile. I think that is really important. There is a whole suite of things and a whole village that has to work together to be able to make that happen.

People have to be more educated on how digital systems work. They have to take up their rights. They have to push companies. Regulators have to be on their game. I think politicians have to support new changes to the law if that is what we need. We also need to give GDPR a chance because it provides all kinds of new powers for us, including our ability to look at

algorithmic decision making, to push for algorithmic transparency and to look at data protection impact assessments that have significant legal effect on individuals. This is a game-changer in terms of legislation, and I would like to be optimistic.

Q940 **Paul Farrelly:** In respect of David Carroll's inquiry, you used the phrase "on point". Here, that is a ballet term. I do not want that to get lost in translation. What did you mean by that?

Elizabeth Denham: I mean that it is a subject of inquiry. His concerns are in line with our concerns. People need to know the provenance and the source of the data and information that is used to make decisions about the receipt of messages. We are really looking at—it is a data audit. That is really what we are carrying out.

Q941 **Paul Farrelly:** So to use a Vancouver term, you're both paddling the same canoe.

Elizabeth Denham: We're paddling in the same canoe. We're rowing in the same direction.

Q942 **Chair:** Could you just explain how you came to have jurisdictional responsibilities in David Carroll's case?

Elizabeth Denham: Because his data was being processed in the UK by Cambridge Analytica, and the Data Protection Act 1998, the GDPR that follows it and the Data Protection Bill do not make distinctions as to citizenship. It does not matter that he is a US citizen; his data are being processed in the UK, so it falls under our jurisdiction.

Chair: Thank you very much. I think that concludes our questions. Thank you very much for your evidence.