HOUSE OF LORDS

Select Committee on Democracy and Digital Technologies

Corrected oral evidence: Democracy and Digital Technologies

Tuesday 4 February 2020

10.10 am

Watch the meeting

Members present: Lord Puttnam (The Chair); Lord Black of Brentwood; Lord German; Lord Harris of Haringey; Lord Holmes of Richmond; Baroness Kidron; Lord Lipsey; Lord Lucas; Lord Knight of Weymouth; Baroness Morris of Yardley.

Evidence Session No. 9	Heard in Public	Questions 112 - 123

Witnesses

I: Ben Scott, Director of Policy and Advocacy, Luminate; Elisabeth Braw, Senior Research Fellow, Royal United Services Institute (RUSI); Lisa-Maria Neudert, Commission Secretary, Oxford Technology and Elections Commission (OxTEC); Paddy McGuinness, Commissioner, OxTEC, and Former Deputy National Security Adviser (2014-18).

Examination of Witnesses

Ben Scott, Elisabeth Braw, Lisa-Maria Neudert and Paddy McGuinness.

Q112 **The Chair:** Good morning and thank you all for joining us. Before I ask you to introduce yourselves, I am obliged to read out the following, which is pretty self-evident. As you will know, this session is open to the public. The webcast of the session goes out live and is subsequently accessible via the parliamentary website. A verbatim transcript will be taken of your evidence and put on the parliamentary website. You will have the opportunity to make minor corrections, for the purposes of clarification or accuracy. Perhaps you would like to introduce yourselves, and then we will get to the first question.

Elisabeth Braw: I am a senior research fellow at RUSI and I lead the modern deterrence project there.

Ben Scott: I direct policy and advocacy for Luminate, which is the London-based part of a charity run by Pierre Omidyar.

Lisa-Maria Neudert: I am a doctoral candidate at the Oxford Internet Institute and a researcher there. Most recently, I served as the secretary to the Oxford Technology and Elections Commission.

Paddy McGuinness: I was a commissioner on this commission of the Oxford Internet Institute. I am a senior adviser at Brunswick Group, which is a critical issues firm. Previously, I was the UK's deputy National Security Adviser, leading on resilience, security and intelligence, including the security of elections and the democratic process.

Q113 **Lord Harris of Haringey:** We have received written evidence from the Government that tells us that, to date, there has not been any evidence of "successful interference in UK democratic processes". I would be interested in hearing your views on the extent to which we should be concerned about foreign interference in UK elections. How resilient are our democratic institutions against interference, perhaps against the use of dark money from malign actors?

Elisabeth Braw: Thank you for that question. It does not actually matter whether interference has taken place if the public discourse suggests that it has. Look at the United States, for example. It is disputed or hotly debated whether Russia influenced the 2016 election, to what extent it did or to what end. What matters is that Americans think the Russians did interfere with the election. A poll by YouGov in the *Economist* in 2018 showed that 50% of Americans think the Russians interfered with the 2016 elections, which is a frightening figure. It does not really matter whether they did; Americans believe they did.

Ben Scott: The absence of evidence is not evidence of absence. We have to recognise the growing sophistication of organised actors who would interfere in elections. The playbook from 2016, which I watched as part of Mrs Clinton's presidential campaign, was a very clumsy, overt attempt at interference. Buying ads with roubles is not covert intelligence activity.

It is shameless, brazen interference in another country's election. What we are seeing now is a lot more sophisticated. It is not the purchase of Facebook advertisements through the front door, using roubles and an address in St Petersburg. You are now seeing dark money, channelled through different shell organisations, paid to PR organisations that set up inauthentic accounts on social media, by the hundreds.

For example, in the recent European parliamentary elections last spring, some entity set up thousands of false Facebook accounts in Germany and used them to amplify and expand the reach of content from a single political party in the German election. It was out in the open and obvious to anyone paying attention. The research community spotted it but, notably, Facebook did not. If the German intelligence agencies and law enforcement officials spotted it, they did not shut it down. It resulted in a substantial increase in the visibility of one party over the others, through deceptive and illegitimate means. I think we will see these kinds of techniques more and more. Money will be paid to third parties to generate artificial traffic on social media, which gives certain voices more volume and prominence in the public debate than they actually represent. That is a dangerous form of influence, because of not only its actual influence, but the perception among the public that the integrity of democracy has weakened.

Lisa-Maria Neudert: When we think about the impact of disinformation and interference, it is a misconception always to think of impact on behaviour. Does it have an impact on how people have voted or the views they have on a certain political issue? It is more often about not just behaviour, but perception. How do the public perceive the pillars of democracy right now? How do the public perceive our elections? Is there electoral integrity? Are our elections free and fair? Is there still truth and trust in the political system? That can be undermined. It is exactly what the Russian and many other foreign playbooks are trying to target. It is not about disseminating a specific message, but more about sowing distrust in institutions and the political system in general.

To the question of how resilient democracies are to that, any democracy will have some form of conflict or issue. That is exactly where disinformation techniques start their narratives. You have a divisive topic and division within the public. It could be a Brexit referendum, a Scottish referendum or questions around immigration. Then you have a foreign or malicious actor disseminating stories about that, often to both sides of the political spectrum, to foster more distrust and public confusion.

Paddy McGuinness: I differ slightly. First, I would like to frame this slightly for the Committee. It seems important to me, as someone from the national security world—a securocrat, I suppose, for most of my professional life—that we understand where this sits in the hierarchy of techniques that a foreign state, say Russia, can bring to bear. We need to understand that, when we think about the digital space, this is the least and the easiest of their tactics. You could divide them into three. At the height are what might be called quasi-kinetic military weapons. They are things you would use in a strategic conflict to have an effect on an opponent. You would be trying to interfere with network systems in the way that you might with a bomb or an electromagnetic pulse weapon. That is kept deeply hidden and rarely brought out and shown. It is really valued by a military-dominated hierarchy such as Russia.

Secondly, you have a set of covert-action techniques that leave firm fingerprints and have real-world effect. They make machines behave differently. You might use them to interfere with Ukraine's power supply or whatever it might be. You will use those in peacetime. You might use them around significant political events or even consider using them against automated or networked voting systems. When we think about interference, we have to be clear what we are talking about. In this country, we vote on paper, but the United States does not. That opens up a whole vista of difficulty. You only have to look at Iowa today to understand that.

Then you get into this area. I remember when we were working against terrorists, and I am happy to talk about this even though we are not in a classified arena, because the Government have done so. Over the years, we have worked against terrorists, and al-Qaeda and Islamic State have been active online. I remember working against them, and military colleagues in the Ministry of Defence talking about this as "messing about on the internet": we were having some effect on the terrorists, but it was nothing like you could have with a quasi-kinetic network weapon. We need to understand where this sits in the hierarchy.

The significance of what the Russians have done, or do, around elections is the intent and the high-handedness of the Russian regime. They understand where the threshold is for intervention and conflict, and stay well below it. Then they give their agencies free rein, which is why you end up with not one but two Russian agencies hacking the Democratic National Convention. No disciplined governmental system would do that, because it is a waste of capability.

There are two other points. I am disturbed by the idea that we are internet zombies. There is an exaggeration of the effect that can be had through network systems upon our intent. Some can be had, but I am very sceptical. If we accept the premise that something profound can be done to all, the majority or a significant number of us, simply by manipulating messages to us based on our Facebook likes, I am really disturbed by the idea, because it delegitimises the vote. It is something we have to avoid. I am happy to go into more detail on that.

This brings me to my third point. We must not do the Russians' work for them. I would love to be a GRU officer responsible for these campaigns, because the success threshold is really low. All I have to do is put you a little more off-balance at a time when you are vulnerable, and you are particularly vulnerable during an election. One reason that the Oxford commission consciously turned away from the threat story, which understandably you started with, and got into the resilience story is that we wanted to define what we, as a society, can do for ourselves to reduce any malign effect. By concentrating on the threat, we talk up the Russians. We make them 10 feet tall. We increase the perception that our elections are vulnerable and may not be legitimate. The reality is that they can have very little effect on us. Sadly, there is a bit of a conspiracy of silence around the true ability to have an effect through network systems, because it is profoundly not in the interest of the advertising industry to admit how little effect can be had, how much they are communicating with botnets and not with human beings, and how few of us are truly influenced to do something we do not really mean to do by what they sell and what they pay social media platforms for. We need to be quite sceptical.

Lord Harris of Haringey: Can I follow up, because this is quite important? You are telling us that, first, we should not be internet zombies but, secondly, the Government's test of whether it is successful interference is the wrong test, under any circumstances. The question is not whether a result was changed, but whether there is confidence in it. If that is the case, what are the appropriate responses, given that this is all driven by social media and digital technologies? What is the appropriate response from the UK Government or any nation state to protect people's feelings that their democracy has integrity?

Elisabeth Braw: I think it is to involve the population. I worry when we have these investigations that show that the Government should do more to protect voting machines and the software in systems. I must congratulate the Committee on scheduling this hearing for today. I know you thought about when the Iowa caucus would be taking place and scheduled it accordingly. This is a perfect example of election interference: we do not know what happened to the apps that the Democrats used in Iowa, but everybody's first assumption or fear is that somebody hacked them. It could be just that an inept IT company developed it, but now we are already worrying about the legitimacy of the outcome of the Democratic nomination in Iowa.

To go back to your question, Lord Harris, a good example is what Latvia does. Latvia is a small country; what can it do to protect itself? It has a national security curriculum that is being rolled out to all senior or high schools in the country, where kids are taught what the threats are facing the country, what the Government do to protect the country and what they can do themselves. If we are not taught about that as citizens, our instinct will always be to think that the Government can somehow put up a more powerful or larger umbrella over us, so that we do not have to worry about this or that threat. The Government cannot do that; they do not have enough resources or money, and it would be a complete waste of the phenomenal resource that is the population. We can actually play a role. It would be a waste to assume that the Government could or should do something.

The Chair: I am eager that we don't try to make life easier for ourselves by looking at Russia as the sole arch-enemy in all this. We are looking at lots of potentially malicious players and I'm eager we don't get overly obsessed with Russia.

Q114 **Baroness Kidron:** I have to make an additional declaration. I work with Luminate and Ben on occasion, and I have a historic connection with Brunswick. I have an additional question. In an attention economy, where do commercial interests and the interests of bad actors coalesce? Could you unpick that a little?

Lisa-Maria Neudert: That is a wonderful question. Does interference always have to be foreign? Does it have to come from malicious actors? When we are looking at this attention economy, we see that the type of information we label as divisive information or disinformation is often the information that reaches most people. In fact, we at the Oxford Internet Institute have just studied the UK elections, and collected millions of tweets and Facebook interactions. We saw that the spread of what we are calling junk news or disinformation is going down overall, but we still see individual pieces of junk news or disinformation widely outperforming professional news. During elections here in the UK, users interacted much more with the junk news than with factual and professional information. That is one of the important takeaways that we should consider today. Interference is not just worrying, but very widespread. We have seen many home-grown alternative news outlets propagating disinformation.

At the same time, we see in Europe, the US and many western democracies parties and mainstream actors taking to very similar techniques, whether disinformation, deceptive campaigning or not disclosing campaign spending accurately. That is happening in broad daylight. Right now in the UK, we have a good framework for regulation, but it is not fit for the digital context. That starts when we are thinking about how spending on digital advertising is reported to the Electoral Commission. We do not have the fine-grain categories we need. Instead, we have a big lump-sum category of digital spending. We do not know whether it was spent on Facebook, Google or Twitter. What kind of advertising was it spent on? Were data provided by the platform or a third-party agency? We need to address those questions to make sure our systems are fit for the digital age.

Q115 **The Chair:** Mr McGuiness, taking your three categorisation, let’s talk about the lower one. We were told last week about the impersonation of the BBC, the *Yorkshire Post* and the Sheffield *Star* online. How seriously should we be concerned and, if our first line of defence is the Electoral Commission, how empowered should it become?

Paddy McGuinness: Thank you very much; that is a really helpful question. On the previous question, having been inside it, it is problematic for a Government to protect this area. Sitting at the green baize table of the National Security Council, it is notable that, when you begin to talk about elections or electoral processes, suddenly everyone looks a little shifty and uncomfortable, because they are parti pris and have to declare their interest, as you deal with it. This is why we need a focus elsewhere and why it is so important that we steer it elsewhere, which we tried to do with the Oxford commission.

We found that there is a set of bodies that have either actual regulatory powers, as the UK Electoral Commission does, in a sense, or what I call uncertainty regulatory powers. In other words, they have real regulatory powers within the sector and, if they say, "It would be really nice if", the sector pays them a bit of attention, so there is a second category of ways in which people can act. There are some bodies there. They are probably not staffed and funded as they need to be but, critically, they are not animated as they need to be. Bodies such as this tend to be animated by government. It is government interaction that drives them along. In this case, government do not interact; they stand back and say, "This is an election and we are elected representatives. We cannot really engage". There is a problem with that, which is why we need to stimulate the behaviour of the Electoral Commission and some other bodies to take a more active role, without direction from government. It should be that way, but it is not. That is the reality. We need to make sure they are resourced.

On the question of what an individual piece means, I remember a conversation with Google. They did a good thing on YouTube, when they removed a set of postings that clearly had been generated by the Russian state. In those, a Russia Today product around the Scottish referendum, if I am not mistaken—I need to check that—had been posted and rebadged as BBC. They said, "Look at this". You could have run forward with that and said that the Scottish referendum was being undermined. There had been 3,000 or 4,000 views, the significant majority of which were the people who had put it up checking it was there. Almost nobody had seen it. It was hard to say that it had had a significant effect on a significant number of people voting.

We need a mechanism that allows an independent body such as the Electoral Commission to make a judgment about whether the intervention is so severe that it has the same kind of effect as misspending funds. The Electoral Commission can say, "I am sorry; this election in this constituency is no good. It has been ruined. We will have to run it again and you are disbarred", or it can fine individuals, but not cancel the election. It does that on financial grounds, not on whether there has been some illicit attempt at interference. The difficulty is finding that threshold. We have a mechanism to judge whether an election is unacceptable in an individual constituency. It is just that we have not loaded this task into it.

Ben Scott: I want to pick up on this point that Mr McGuinness has raised about assessment of impact, because it is the centre of the problem. You cannot assess the impact. Let us take the Russians as one among many actors in a complex system. That is fundamentally driven by a logic not of providing information to voters, but of providing audiences to advertisers. This is the commercial model that sits at the base of social media.

I will use the example of what may happen today in Iowa, since it is fresh in the news. It is not difficult to imagine that results are declared later today, and disappointed losers and their followers begin to spread a conspiracy theory about hacking of the results tabulation in the Iowa caucuses. If that does not happen, I would be surprised. That conspiracy theory might be motivated and generated by disappointed voters who have no connection to any kind of organised attempt to undermine the legitimacy of the American election. However, once it begins to take hold, it will become popular because conspiracy theories are popular. Under the logic of the journalistic commercial media system, responsible editors would not print a conspiracy theory that has no factual evidence underneath it. It will not appear on the front page of the *Des Moines Register*. It will not be a headline on the local broadcast television news in Iowa City, unless it is to debunk that conspiracy as false.

Flash over to social media—YouTube, Facebook, Instagram or Twitter. That conspiracy theory will go like wildfire. Why will it? The purpose of the editorial function on social media is not to provide factual information to citizens or even to pretend to; it is to get people to look at more ads. Whatever it is that gets you to look at more ads is what they are going to serve you. If a conspiracy theory about the illegitimacy of the Iowa caucuses sells ads, you can bet your bottom dollar that will fly around social media at 10 times the rate of any truth statement about the evidence underneath it.

Then the Russians come along and all they have to do is nudge. Was the Russian intervention that amplified the conspiracy theory by 5%, 2% or 6% impactful? Was it definitive? Did it turn the tables? I do not know. No one can, but we know that the spread of disinformation for the purpose of monetising advertising is a pernicious force. We can determine that for sure from the last several years. When we shine a regulatory light on it to begin to identify and remedy such a problem, we cannot see the data. We can only see the individual instances.

We see incident reports. "Look, here is a screenshot of a tweet of someone spreading a conspiracy. Look, here is a YouTube video that YouTube took down because it was so obviously made by a bad actor". What about the 10,000 other pieces of content that have circulated? What about all the people who shared those, innocently thinking that they were legitimate? Do we have the data to reconcile them and assess their impact on the voting public? We do not. Do the companies have that data? Absolutely they do. Why do we not have access to that data in any kind of oversight capacity? No other industry that has this kind of impact on the public would be able to say, "Trust me; everything is fine. Don't worry". This is the fundamental issue that we have to get at when we are talking about how to assess the impact of the problem.

Elisabeth Braw: Following what Ben said, this is why it comes down to involving the population. If I may quote the famous Austrian novelist Stefan Zweig, he writes in his autobiography a sentence that applies very much to this. It is about Vienna at the beginning of the 20th century. He writes, "They drowsed their lives away", and that very much applies to us today. We lazily spread content that we should not be spreading. Yes, there should be more regulation of the technology companies that make money from it and rather unethically help it spread. But what if we starved the problem of oxygen from the other side, by empowering people and educating them about the damage they do to our own system, in whatever liberal democracy it is, by sharing that information? If we starve it of oxygen from both sides, we will have a good chance of at least minimising, if not eliminating, the problem.

Paddy McGuinness: I have two thoughts. I strongly agree with Ben that transparency is the route through this. It cannot be to trust the companies, the political parties, the advertising industry or indeed the media. It must be to trust and verify. That leads you to the question of who the verifiers are. For me, one of the most disturbing aspects of the debate in the last general election here was when an Intelligence and Security Committee report was not released and everyone said, "Oh, it is dreadful; it has not been released". What kind of country are we if we need our intelligence agencies to tell us whether our elections are valid? They are fine organisations, but it must be for non-state organisations to tell us. Non-state organisations, such as those represented here, should tell us what is in the data and what is happening.

You can see that I disagree with Ben about the effect. We do not know what effect has been had through this. Anecdotally, little effect is had because, while conspiracy theories go wide, how they are read depends. Is it believed or do people just say, "Look, there is a great story. It is not true, of course"? I remember the front page of the *Observer* before it had photographs. The top story was always one that was not quite true. It was convenient, because you knew where it was. It was always a good story, but not true. That is how I see my teenage children reading the internet. There is an interesting question about where we put our effort. Is it into civics and critical reading of what is received, or trying to restrict what is distributed, which may be a finger in the dyke?

Q116 **Lord Lipsey:** I am a bit of a Paddy-ist on this one. Over 40 years ago, I was a special adviser in the Foreign Office, which had a special department called the IRD, set up with the sole purpose of distributing anti-communist propaganda, not approved by Ministers, around the world, unattributed. I would not say it had no effect. It had the effect of producing, for the left of the Labour Party, an argument to show that the state was deeply anti any form of socialism. Otherwise it was a complete waste of time and effort, and I suspect the same may be true of this. I take the point that no evidence is not the same as something not being the case, but the fact is that all the academic studies show no influence on voting behaviour. It is very implausible that it would have an effect on other things. It is sort of Mr Putin's toy. For little money, the Russians can impress their President with their sophistication, but there is not much sign of impact. I wonder if anyone has a killing argument as to why I am wrong. If we are to deal with this, are there any propositions, further to Paddy's to leave this to non-state organisations? Does anyone believe that we should have some sort of state or regulatory intervention to try to prevent this stuff?

Lisa-Maria Neudert: When we think about impact, we often talk about the impact on the wider population, but impact can also be very narrow.

It can be enough for a piece of disinformation or a certain campaign to convince just a handful or even one individual. As a recent example, the World Health Organization is currently co-operating with Google to bring out public health information on conspiracy theories and disinformation about coronavirus. The most popular theories that have been spreading are that you can vaccinate yourself against coronavirus by inhaling sulphurous fumes from fireworks and that you can use garlic to protect yourself from coronavirus, which is obviously very wrong. To stick with epidemiology, it is enough for one person to believe that. If one person thinks, "I can actually vaccinate myself by inhaling a firework", there will be a terrible health effect no matter what. If that person then contracts coronavirus, because he thinks he cannot get it, and spreads it, we have a real-world impact from a piece of disinformation. In this analogy, we have a disease that is arguably spreading just as quickly as disinformation.

It does not take a lot of people. It is enough to have one lunatic in Washington DC, who thinks there is a pizza joint actually running a child pornography ring for Hillary Clinton, to go into that establishment shooting innocent people. It is the same if a handful of people believe they can vaccinate themselves against coronavirus this way. Disinformation stories have many other implications. You do not need a range of the wider populace but, if you have a couple of people who are really convinced, the thing can catch on.

Ben Scott: I would like to take up the challenge from Lord Lipsey and argue that you are wrong. The reason you are wrong necessarily leads to a regulatory solution. Premise 1 is that you will never find evidence that a single piece of communication in the mass media has an influence on mass participation at the voting booth. Never, in the history of communication study, has anyone ever been able to prove quantitively that there was a strong media effect from a direct transmission of one communication to one small part of the audience. It is the bane of the advertising industry's existence that it cannot quantify this. It does know that, if it stops advertising, market share declines relative to competitors that do advertise. No one is quite sure why it is that certain communications end up causing attitude change in the public, when others do not.

The mystery of how to quantify media effects has bedevilled communications researchers for decades. I studied in my graduate school days at the Institute of Communications Research at the University of Illinois, which was set up by the CIA in the 1950s to study propaganda lobbed over the Iron Curtain. It came up with no compelling evidence that this was effective, and yet continued to do so, because it knew of no other way to continue to influence the audience it was targeting.

However, we now live in an environment where the theory of communications effects must be understood as systemic. They happen gradually and cumulatively over time and are very difficult to measure, particularly in an environment where the average individual consumes thousands of pieces of information every day, scrolling across screens at a rate of several per second. Why do large chunks of our population believe in total fantasy, such as the anti-vax conspiracy? Why does a large chunk of the American public continue to believe that Barack Obama was not born in the United States or that he is a secret Muslim? Why can we not solve any of the grand challenges of today, whether climate change or migration; because so many of our fellow citizens believe in things that are demonstrably untrue? We cannot route those beliefs to any particular campaign of disinformation. We can only see that they are having an impact systemically.

Secondly, if you speak to the experts in artificial intelligence and machine learning, who are developing theories at the cutting edge of how data are processed in social media companies, they will argue with great confidence that not only is artificial intelligence that targets information at individuals successful at maximising their attention, but it is successful in changing their attitudes and views to make them an easier target for maximising attention. They are able to change the way people think to make them more inclined to look at extremist and conspiratorial content, because that makes it easier to sell them more ads.

Now, if either of my premises might be true, we have an obligation as a democratic society to try to find out. That is my argument. If you believe that either of those things could be true and that all the scientists in the AI field could be right that social media has this kind of impact, but we cannot measure it without an extraordinarily careful study of the data, we need to take one first step in the regulatory arena. We need to pry open the lid of the private sector's hoarded data supply, so that researchers, such as those either side of me, can evaluate that data and determine whether we can say, one way or the other, that the impact is weak or strong. It may have no impact at all, but the fact that we do not know, that it might have a strong impact and that credible experts believe it does, suggests that we must have a look.

Lord Lipsey: It does not seem that you are contradicting me at all. I totally agree that we must keep looking at this stuff and testing whether it is effective. Time alone will tell whether those of us who do not believe it has a compelling effect, or those who believe it has a serious effect, are right. This is not a disagreement. Yes, we want to go on researching.

Ben Scott: To do that research requires law, because the companies will not voluntarily make their data available.

Elisabeth Braw: Lord Lipsey, I agree with you, but the point of the various interference attempts, which may or may not have happened, is not whether or to what extent they were successful, but the perception that they happened and were successful. If you are a malicious actor, if you give the impression of interfering in another country's election, your work is already done, whether you were successful or not. That comes down to a point that was raised by Lord Puttnam's namesake Robert Putnam in 2000, in a book called *Bowling Alone*, with which I am sure you are all familiar. Professor Putnam was prophetic in pointing out the risks of decline in civic participation, because the more atomised or fragmented societies become, the more likely we are to believe negative things about our fellow citizens. That was not the point he made in 2000; he just documented the decline of civic participation in the US. Of course, the trend is similar in other countries. That has now become a national security issue, because it provides a whole new front for countries and other malicious actors that want to weaken our societies.

Paddy McGuinness: I have three quick points. The first is to cap off the thing about state actors. Initial interference of this kind is a slight indication of their overall intent. If one thinks about where to put one's effort, there is a national security effort to stop them at the game line in this kind of activity, so that we do not find them, as we did in 2016, on 500,000 telephony routers, for whatever purpose—Huawei and others—messing with our communication systems. That is an area of state competition and the beginnings of their reconnaissance. Absolutely, we should stop them on the game line and have the means to do so.

Secondly, I agree with Ben that we are not going to get to a place where the non-state can manage this and we have true transparency, if there is no regulation, law or means of pressure. That is true of the social media companies and I believe it is true of the political parties. We need to understand what the political parties are doing, not least their intent. As you raised earlier, there is the issue of funding. You begin to be concerned about a state interfering through not the data in an election but the money in an election. You might be concerned in Germany, for instance. Then you need to understand what the party thus funded is doing and whether it is sinister. That is vital.

The third point was made very clearly by Lisa. It is now true that, when we have a significant crisis or event—I will give you two: we have talked about coronavirus, but there is also COP 26—we need to set ourselves, both government and non-government, to defend that against being delegitimised, which there is a definite effort to do. We can do that by shining a light brightly and transparently on what people are doing around it, so we can have the proper discourse Ben talked about to resolve the problems.

Q117 **The Chair:** Ms Neudert, this begs a question that Mr McGuiness and Mr Scott have raised. With the political system we have in this country, when many of these issues are not provable, what levers can you use to get Governments—that is to say, of all political parties—to accept that they have to come up with legislation that might be inconvenient to them, in a sense? Mr McGuiness, is that simply a way of re-expressing what you've just said?

Paddy McGuinness: No; I think you are saying a different thing, but I think it is valuable.

The Chair: I'll settle for that!

Lisa-Maria Neudert: I think you are asking whether we have the data to say we need regulatory intervention.

The Chair: In a data vacuum, which is to a degree what we’re looking at, while we understand the problem—Mr Scott explained it extremely well—how do you get political actors to take an important decision to legitimise politics, when it could be said to be against their immediate self-interest?

Lisa-Maria Neudert: On the one hand, we have citizens, leading academics and many people in government shouting from the top of their lungs that we need more evidence. We are arguably already in a moment of crisis, when we are looking at social media and platforms. For the report that OxTEC published in October, we interviewed several stakeholders and public agencies, such as the ICO and Electoral Commission, and many stakeholders in civil society, from journalists to watchdogs and civic society organisations. There has been boggling agreement that we do not quite understand social media yet. There are many incentives coming together. Ben has eloquently spoken about the advertising sector, which is a huge incentive, but there are also social incentives for people to post dubious disinformation on social media. We have political incentives to do that and we can see many stakeholders in the UK and around the globe using that, right now.

Yes, we do not know the impact. We also do not have a definite statement on spread. When we are looking at the spread of data that researchers would like, it is just a public spread. There is much more of that kind of disinformation spreading in non-public groups and WhatsApp groups, where this kind of content is still dominant. What we are asking for—and everyone is looking at politics for help—is just the tip of the iceberg: to get information from platforms, which they are analysing with questions about how well advertising performs, and to analyse it with questions about how we should protect democracy.

Q118 **Baroness Morris of Yardley:** It is clearly a very complicated area. You have already talked about what the different parts of the system can do to try to solve the problem. This question is really about digital literacy. Within the context that you have already spoken about, what can we expect of the citizen? How big a role can they play if we get better at digital literacy? That includes an understanding of information processing. Do you have any examples of how this could be done and what we might do to achieve it? What could the extent of our ambition be?

Lisa-Maria Neudert: You are absolutely right. Again, the example of Latvia is excellent. It involves every teenager. This may be an imperfect analogy, but remember the problem of internet predators a few years ago. It was a huge problem: you cannot stop them from being on the internet; the police can do undercover stings and so forth, but the problem persists. Instead, various levels of government and NGOs trained kids not to engage with suspicious people online. That was hugely successful; I think we can all agree. That may be imperfect, but it is a workable analogy of what can be done with democracy.

We have a captive audience of teenagers and younger preteens even, who can be taught about the malign activity that goes on, on the internet, with not just internet predators but hostile state actors. I look at the curriculum in England, and I know it is difficult to change. In PHSE, my teenagers learn about body image. Why can they not learn about what other countries and malign actors are doing to a country such as this? Once they know what is happening and are equipped not to share information without informing themselves about where it comes from and whether it is credible, they can communicate that skill to their parents. If we are to involve society, schoolkids would be a good place to start.

Ben Scott: I agree. In my role as a foundation officer, I have invested in experimental digital literacy programmes from all around the world looking at exactly how we do this. It is a nascent field. As a director of one of the best programmes said to me, "If you had an hour with every 16 year-old in the country to change how they think about social media and democracy, what would you say?" What could you say that would possibly stick with them and give them something to take away from the classroom that would change the way they behave on the internet? That is a very difficult problem and one that will take a long time to work out. It will take steady interventions, but there are some interesting data points.

Elisabeth pointed to what is happening in Latvia. Finland is another interesting case that is often held up. The Finns essentially ran a public service campaign on every state-owned media channel, which most private sector media channels got on board with, saying that it was the patriotic duty of every Finnish citizen to tell the difference between truth and falsehood online, because the Russians were coming for them. That was a very successful campaign. Now, that is a small country in a very closed language market. They have unusual geopolitics; nonetheless, it is instructive.

Let me back out for a moment and suggest why we have such a big challenge. It is hard for those of us who were socialised into the media system prior to the internet to understand what it is like to be part of the digital-native generation. When I talk to my children about this, I see it. When you walked into a newsagent at the airport 25 years ago, before you were even close enough to the periodicals rack to see the titles, you more or less knew what you were going to get. You knew because the store is organised in a particular way. By the registers are the daily broadsheets. They are printed on a certain kind of paper. The ratio of image to text is a certain way. The size of the font and the flair of the headline give you a sense of what kind of paper it is.

You have a set of associations with the brands and how hard they have worked to be seen as quality, credible, right-leaning or left-leaning. When you go to the periodical wall, you know they are going to be divided by subject matter and, before you pick something up, you more or less know what you are going to get. You will adjust your view based on what you read on the front page when you get it. Those are normative cues about quality and credibility that sort in your mind, in advance of information consumption, how to think about it and where to place it in your hierarchy of credibility.

Now think about Facebook, Twitter, Google search results or a series of YouTube videos that flow across your screen. They are all compressed into a single feed. They are all made to look the same. They are surrounded by a blue box. They are written in the same font. At the moment that you consume it, you may notice that a story came from the BBC or the *Daily Telegraph*. The next day, when you tell your friend what you read on the internet, they ask, "Where did you see that?" You say, "I read it on Facebook". "But you did not read it on Facebook; you read it somewhere through Facebook. What was the source?" "I don't remember". "Was it a quality source? Was it a credible source?" "I have no idea". That is how we, as a society, lose our connection to the rudder, which is a common understanding of the factual presentation of the world around us. That is why we are seeing all this fragmentation and polarisation. We have lost connection with a common sense of the world around us, on which we can deliberate, compromise and move forward as countries.

Lisa-Maria Neudert: I have a slightly more pessimistic view on digital media literacy for two main reasons. First, thinking about the digital landscape right now, we have artificial intelligence and sophisticated fake material coming in. We can automatically produce convincing video and text, which looks very credible. It is credible to the extent that it takes expert fact-checkers several hours a day to identify whether a video was faked or artificially generated. Now imagine you are asking the average user to do the same thing. That is an incredibly big question and you need an incredibly difficult toolset to assess it. In thinking of just digital literacy, we are putting a lot of onus on the citizen.

Secondly, when we look into what kind of disinformation is doing very well on social media, it is often not the sophisticated stuff. It is often the stuff that is demonstrably false, the crazy conspiracy theory. If you google it, you will have a ton of debunking stories about it already. Even if you look at the comments section, a lot of people will be saying, "Obviously this is not what is going on", but we have something called confirmation bias. People want to believe narratives that fit their existing belief system. If people already believe that the BBC and the Government are putting out disinformation and are not to be trusted, when they read a story that fits that narrative, this is exactly how disinformation works.

Digital literacy is about how people assess information and the quality of that information, but there is another door to it, which is cybersecurity. Right now, we are looking into the curricula and how the public are talking about digital literacy, and there is not much room for cybersecurity. What do I mean by cybersecurity? There are very simple protocols, for example how to keep a password manager and how to make your online communication safe. There are simple tools that are easily accessible. No matter what, I think they would make a big difference. For example, one of the biggest disinformation stories and impacts over the past couple of years was the hack of the DNC. That could easily have been avoided if we had password-protected, safe communication online. It is not just about how teenagers are getting information from social media, but about how the Government are using cybersecurity at an entry level of capacity, when thinking about digital literacy.

Paddy McGuinness: I want to talk about a slightly different kind of digital literacy but, if you want to stop me, we can discuss it somewhere else.

The Chair: Can we pick up a question from Lord Knight?

Q119 **Lord Knight of Weymouth:** I am afraid this is the first time I have spoken since the Committee was reformed, so I need to declare my interest in respect of my employment at TES Global Ltd. We are a platform provider of user-generated content. I was interested in what you were saying, Mr Scott, following what Elisabeth Braw was saying. You mentioned Finland where, as I understand from reading a media source I choose to trust, schools teach digital literacy across the curriculum. They do not try to squirrel it away in one bit of a non-compulsory part of the curriculum. In maths, they would teach how you can use statistics to tell different stories, for example. You can use digital literacy in history and think about it across the curriculum. Is that a better approach?

There is an additional question on the substantive point that you were both making. Google's last major algorithm change, in March, was about trying to ensure that search results were prioritised according to their expertise, authority and trust. In a way, it feels credible that people at Google, who are training their algorithms and then checking them with humans, would be better at differentiating what is fake than lay people, however educated. How much can or should we be regulating and, in a way, trusting the likes of Google, picking out the best and worst examples, and how much do we then rely on the citizen?

Ben Scott: Integrating digital literacy into existing curricula is the way to go. I have invested in both strategies: stand-alone modules that can be dropped between the gaps of other curricular studies; and programmes that attempt to integrate it into a multi-subject, long-form module. The latter is both more successful and more popular with teachers and students, because they are not asked to digest new material from scratch that is unrelated to anything they have ever taught before. What I have learned in the digital literacy space so far is that, if you do not have the teachers on board, you have nothing. Ultimately, it is not the digital literacy experts who go into the classroom, day after day, and talk to teenagers. The teachers do that. If they are not able to do it comfortably, confidently and effectively, it will fail.

On the Google algorithm point: trust but verify. That is exactly the principle we ought to be driving at here. Imagine, for example, an adjacent industry that we are more familiar with, which is equally complex and has an equally large impact on the public: the pharmaceutical industry. Imagine the pharmaceutical industry said, "We have new cancer drugs, which we are rolling out to the market. They are very effective. We have refined them to be more effective and to reduce the side-effects that our previous generation of cancer drugs had. They are going to be of revolutionary benefit to the public".

We would all say, "That is great. Now we want an independent scientific regulator to go in and verify exactly what is in the bottle that you are peddling to the people. We need an independent review of their effects to make sure what you are saying is accurate. If it is, we will all applaud. Off we will go to deliver those drugs to the people and get the benefits". That regulatory piece is critical to holding companies accountable and cuts against the commercial interests of those who would say one thing and do another.

Elisabeth Braw: Following up on this question and the one from Baroness Morris, another good example I should have mentioned earlier is the brochure that the Swedish Civil Contingencies Agency put out in May 2018. I do not know if any of you heard about this. It is called *If Crisis or War Comes*. It is an A5-sized brochure with bullet points about what to do in all kinds of crises—natural disasters, brazen attacks or an invasion of Sweden. It is very easily accessible information that everybody can understand. It was sent to every household in the country by post, so you do not have to download it. If the internet goes down, obviously you will not be able to download it. As a result, 75% of those who received it read it and that is quite an impressive figure. Disinformation has its own page with bullet points, including whether the source of the information is trustworthy and in whose interest it is to put out this information. Even small points like that make people think about whether they should be passing on information.

This is a completely different example, following Ben's point about teachers. I am an opera fan, and opera houses around the world struggle to bring in young people. They are seen as completely inaccessible; why would you be interested in opera? The opera house in Warsaw started an education programme for teachers, so they could understand what opera is about and why it is relevant. They spread that information to their classrooms, because they became converts. As a result, the Warsaw opera house has phenomenal attendance. Every opera house struggles with attendance, but I was there recently at an extremely avant-garde production. I had to leave in the interval, but there it was, attended by lots of young people. I am not saying that, if we can do it with opera, we can do it with democracy.

The Chair: It could be a great headline!

Elisabeth Braw: You can claim it.

Q120 **Baroness Morris of Yardley:** The examples you have given, Elisabeth and Ben, are excellent. They are optimistic and show that we can do things, so I am with you on that, but there is one thing I worry about that is not clear in my head. In the examples you gave, there was an absolute consequence if the child got it wrong. All children are aware of what can happen with people who treat them badly if they meet them online and they cannot trust them. Do we not have to build the other bit? It is worrying me that I am not sure how many young people will say, "This is really important because, if we do not get this right, democracy is threatened". They have never lived in anything but a democracy. They probably do not have awareness of what is at risk. The prevailing thought at the moment is that our Government are not very good and politics is broken. I am not looking for a long answer, but is that a bit different from the examples you have given?

Elisabeth Braw: It is. I am glad you mentioned that because, as you would have heard, the Cambridge Centre for the Future of Democracy released an extremely interesting and, I think, quite depressing report a few days ago. It shows that, in the UK, the percentage of people dissatisfied with democracy was at a record high of 61% just before the last election. That is up from 33%, so almost a 100% increase in less than two decades. I think that is because people have no idea what it is like not to have democracy. We have been spoilt by having democracy. We do not know what it is like not to have it. It is like good health; you do not appreciate it until you no longer have it, and then it is too late.

If I may make a radical suggestion, all around us are people who have experienced authoritarian regimes or dictatorships. They live all around us here in the UK and other parts of Europe. They are the best possible resource for everybody to find out what it is like not to have democracy any more. Obviously we would not want to experiment with a lack of democracy ourselves, but what if some part of government or local government brought in these people—survivors of the Third Reich and people who lived behind the Iron Curtain—so that ordinary people around the country could hear from them what it is like not to live with democracy? That would make the danger all the clearer to them. It would not bring it down to the personal level of "what an internet predator can do to me", but it would make what is at stake much clearer.

Baroness Morris of Yardley: It makes the link, yes.

Paddy McGuinness: I want to touch on another aspect of digital literacy, which is relevant to what Elisabeth has just been saying. I mean no disrespect to the legislature, and I have been working for the Executive, but we tend to be 10 years behind the curve of what is needed from technology. Some 10 years after Facebook burst on to the scene, we have consideration of internet safety legislation in the Queen's Speech. We are 10 years late. Elisabeth is right to talk about the way in which democracy is affected. A democracy is affected by political movements, but also by technology. There is no denying that.

When thinking about digital literacy, there is a thing that I call the technology risk. I wish I could find a better word than "risk". The healthiest companies—and every company now has a dependency on data or enabling technologies—regularly consider what the changes in technology mean for their business models. If we are going to have a conversation, as we are today, about what to do about elections and democracy—Ben has made this point for us—it must not be based on what we can see in the rear-view mirror. We need a way of doing it that accommodates changes in the available technologies. Even though we may argue about whether artificial intelligence and deep fakes will have a profound effect in the next two or three years, it is very hard to argue about which technology will be doing what to us in the next 10 years, and where we will be with a range of other technologies that will bring information to bear in a different way.

For digital literacy, we need a space where we talk about the effect technology is having on our societies, faster. That is a real challenge for those of us who are not digital natives or not close to the technology industry and paid to do this all the time. That then feeds into what the teacher says to the children. That has to be informed by the technologies that are ahead of the children, not behind them. Personally, I have found that my children have been incredibly well-supervised, and I am really pleased with the way in which they interact with what I call the ephemeral internet, which is the internet they tell me they cannot live without. I am really pleased by the way they interact with that, but I can see that that will be dated by the time they are 25 or 30, and it will be somewhere else. There is a digital literacy point for all of us, not just for young people.

The Chair: It is a great challenge for us. The problem is that there is at least a five-year lag in politically implementing the kind of regulation that could seriously address these things. Our job is to try to short-circuit that five-year lag. That is what we are trying to do.

Paddy McGuinness: One aspect of what Elisabeth raised about educating people about the implications of not living in a democracy is that you come to fear the state. You educate about what authoritarian states do, and say, "We must not have the state interfering in the arenas in which we live out our democratic lives", i.e. online. That is why there is this question of transparency, and not just about what is published. As Lisa rightly said, it is not just what is put in the public domain but the mechanisms that are used and the more hidden areas that need to be transparent—so, non-governmental actors that help you make the case for the kind of regulation or legislation that you need. If you are doing it and it is done by the Secretary of State for Digital, Culture, Media and Sport, it is the state doing something to the people.

Q121 **Lord German:** You have unsurprisingly, throughout the whole discussion, referred to the question that I wanted to ask, which is about the role of civil society non-state actors in creating a resilient society. You have ranged from shouting at the top of your voices to doing education. I would like you to prioritise what the role of civil society non-state actors should be in developing and helping support a resilient democracy. You have already identified lots of things. Which are at the top of your agenda?

Lisa-Maria Neudert: In our OxTEC report that came out in October, we identified three things that civil society can do right now. First, we need civil society to work with the data available through the public domain and, for example, Facebook's advertising archive. Twitter and Google have similar efforts. We can work with that publicly available data and look at what is going on over social media. Secondly, and related to that, we need to identify the type of data we need and advocate for it. We have just established that there will probably be a five-year lag for any sort of regulation coming in, but there is also self-regulation.

We have platforms coming forward with certain amounts of data, transparency information and transparency reports, but often, whether it is an advertising archive or a transparency report, the categories for reporting things are too broad and not really helpful. They are not helpful for research or civil society organisations. For example, Twitter and Facebook might have transparency reports on what kind of information they are taking down and how much, but they are not reporting whether it was taken down because it was illegal speech or against their terms of platform service. Right now, it is a very important role of civil society to lobby and advocate for that kind of information. They are the actors that we are looking to in navigating that dialogue. That needs to happen now, not in five years.

Ben Scott: I will simply agree that research and education are top of the list. The best empirical analysis of what is happening in digital disinformation is in research universities around the world. They need resources and more data to do even more of that kind of work. It is pulling back the curtain on this surveillance commerce that has begun to dominate our information markets. The second thing is education. This reprises our theme of how we train more teachers, giving them the tools they need in the classroom to educate students about how to understand this phenomenon and conduct themselves in this space.

The third thing I would put on the list is a kind of movement-building. How do you change people's attitudes about what they imagine digital media should be, what they expect from the companies that deliver products and services in that market, and what they demand is available to them as citizens in a democracy? We have become conditioned to accept that the digital media landscape will be dominated by two or three companies. Why is that? It was not like that even five years ago.

If I had sat in front of this Committee 10 years ago, I would have argued about what a fantastic force for democratic good in the world the internet is. I did that for the Obama Administration. It was not that long ago that the internet was considered, by and large, a force for progress. What has gone wrong has gone wrong recently and is, in my view, most likely to reverse itself. We are most likely to see that five-year or 10-year lag in government response and market change begin to turn when we see people demand better. People will demand better only if they imagine it is possible and they are given leave to expect better from the companies and Governments that determine how the market behaves. That is something in which we can all play a part.

The Chair: We need to let them know what “better” might look like.

Paddy McGuinness: I am a philosopher’s son, so I will put it to you like this. We need to enable civil society to tell us what the case is. Because we cannot rely on Google to tell us, and many feel you cannot rely on the state to do so, you need a setting based on empirical data, where it is possible for the kinds of institutions that are sat here to say, “We have looked at the data and this is the case”. You can rely on that, but you cannot rely on it fully from any other source, I suggest.

Elisabeth Braw: Civil society includes entrepreneurs and would-be entrepreneurs. In a previous life, I was a technology correspondent based in San Francisco and I cannot tell you how many times I was surprised by the quite marginal products that these very brilliant guys came up with. Some guy had discovered that there was no parking or hotel rooms in San Francisco, so he invented an app for that. If these hugely brilliant young men and women understood the extent of the threat to our democracy that technology poses, we would not just have three companies; lots of new companies would try to address it. Who knows how successful they would be? But at least we would have a larger number of companies out there, hopefully some for good. There is an opportunity to educate these hugely talented entrepreneurs and would-be entrepreneurs about what is needed, so that they do not invent more parking apps. I hope they will no longer be needed anyway, because we will have moved away from a car-based culture.

A second thing is the role of newspapers. A number of years ago, I was a fellow at the Reuters Institute at Oxford, looking at the growing divide between the public and the political media elite. One idea from that research was that newspapers should have surgeries, just like MPs. MPs put themselves at the public’s disposal and tell them what they do, and the public ask questions. The public cannot ask newspaper editors questions and, as a result, they get suspicious about how the news media operate. It would not be a complete answer, but imagine what divide we could bridge by having citizens interact with journalists. As a result, they would trust the mainstream media and resort less to conspiracy-feeding outlets that are definitely harming our democracies.

Lord German: I would love to have that conversation for a bit longer, because the key issue for me, to take the figures Elisabeth raised, is how we go from 61% back to 33% again. What is the first thing you would do about that?

The Chair: Can I return to that as the final question?

Q122 **Lord Lucas:** To be annoying and pick up on what you have just said, what experience do you have of the likes of Delib and citizens.is? It seems that, by working in a successful local digital democracy, they give people a taste for it. It is something that newspapers could use for interaction with their readers. Have you seen anything like that? If we cannot go in a positive direction, how could electoral law, or the role of the Electoral Commission or other regulators, be changed to give us better protection?

Elisabeth Braw: In answer to your first question, the only example I am aware of so far is something that *Der Spiegel* in Germany started last year. It started running surgeries like those I have just described. It would be interesting to hear about the results so far.

Ben Scott: I will make two quick points. First, investing in deliberative civic organisations at the local level is critical. I can tell you, from the perspective of the foundation, that there is simply not enough money in the sector. A number of promising experiments are happening around the world, but they are tiny and the number of people they engage is too small to have a macro impact on public perception.

There is one issue on regulation that I would be remiss not to raise before we conclude. We have been talking about the most difficult problems of both measuring and managing digital disinformation. We have not yet talked about the simplest things we can do. In security terms, we should lock the front door: we should regulate political advertising on digital media. This is very easy to do. It is clear how to do it. There is no mystery about why it needs to be done, yet we have not done it. The consequences, while they have not been severe in the short term, very well could be.

There is no reason in the world why we cannot force all the companies that sell political ads to make them obviously visible as political ads to any reader. There is no reason why they cannot do that in real time. There is no reason why they cannot disclose, after the fact, how much was paid for an ad, who bought it, who was targeted by that ad and how many people it reached, so that everybody is aware of what is happening in terms of paid political communications. That is not being done. Just in the last election, three days before the vote in December, Facebook had a glitch and its self-regulated, publicly available ad database went offline for 36 hours. It offered no explanation or apology. It just shrugged and nobody did anything. We should lock the front door.

Lisa-Maria Neudert: To add to what Ben said, there is a role for political parties. Political parties could disclose what kind of advertising they are putting out online. It does not have to be just Facebook and Google that have an advertising archive for digital material; it could also be the parties. Parties are already archiving their non-online campaign materials, so why not extend that to their online material?

The second thing I want to push is this. Political campaigning is no longer something that just happens during election season. It is a year-round, year-long effort, where we have parties but also other forms of campaigners. We have big pharma and oil companies putting political advertising out over social media. We should rethink that and accordingly rethink the role of many regulators here in the UK, the Electoral Commission for example. That is a consequence we should draw.

Q123 **The Chair:** Thank you very much. I would like to wrap up the questions from Lord Lucas and Lord German in a final question, because you may be able to pull this in. If the Government could do just one thing to improve the resilience of our democracy in a digital age, what would it be? I am afraid we have to keep it pretty short. Paddy, what one thing would you like to see?

Paddy McGuinness: I am torn, because I have two.

The Chair: Okay, you are allowed.

Paddy McGuinness: Thank you very much. We did a whole load of work on this and we have produced a report that we will submit with a set of recommendations, which were very specific and designed to be available to the United Kingdom in 2019. They are very specific things you can do but, broadly speaking, I will say two things. First, you could regulate and also use existing regulation to drive the availability of data for transparency, so that you have the reflecting mirror of non-governmental organisations and academia, and you really know what is the case.

Secondly, we could galvanise our existing institutions. We have talked about the Electoral Commission, but others have a role, including the police service when one gets into more criminal areas. When we look at it, all these bodies have a potential role in protecting democracy, but they are not terribly active in it, because there is no animus at its core. There is something about how you animate those groups, which meet informally, and make them meet and act formally, conscious that they are protecting democracy, but not as a function of the Executive. It is a bit of a challenge, but it is what I want.

Lisa-Maria Neudert: To put it very bluntly, it is to make the frameworks that we have fit for the digital context. We have good frameworks, good regulators and many existing regulations on elections, democracy and political campaigning, but now we need to look at how to make them fit for the digital context. That includes political advertising on platforms, how information is spreading over social media and the scale. Scale is one of the important things we need to think about. We see billions of pieces of information over social media and the internet every day and, for that, we need new approaches to thinking about them, monitoring that and government’s role in this process.

The Chair: I wrote on behalf of the Committee to the Cabinet Secretary, immediately before the election, asking what action the Government would take in the event of a contested election result in Britain. There really was no clear answer. It seems to me that we do not have a policy or process, that takes account of such an event, which is extraordinary. Answering with the Iowa non-result in mind, what one thing would you like to see us do?

Ben Scott: I could say many things, but I would argue that all roads lead back to one: audit. The public must have the ability to audit those industries that control the flow of information to society, which is opaque and held proprietary by a small number of companies that are more powerful than any in the history of the media system in the world. We must be able to audit them. We must be able to send in expert researchers, who are independent of the company, to review exactly what is going on in those systems and how influential they are in spreading disinformation from foreign operations, in hiding the flow of dark money in our elections, and in propagating the organised effort to deceive and promote inauthentic content to an unsuspecting public. All these things can be measured, ferreted out and eliminated only through oversight, and oversight requires audit, with mandatory access to data.

Elisabeth Braw: Unlike Ben, I think all roads lead to citizens' engagement, even though I do not dispute what Ben said. The first step I would like to see, as pedestrian as it may sound, is a brochure like that put out by the Swedish Civil Contingencies Agency, but with the title, "Why Election Security Matters to You". Once equipped with that information, most people would have a better understanding of why elections or democracy as such are not abstract concepts, but concern them directly and rely on their active engagement. Based on that, one could follow up with various forms of engagement, including bringing in people who have experienced or lived through dictatorships in authoritarian countries. But it starts there. I think it would get some thinking going among the 61% who are dissatisfied with democracy.

The Chair: Thank you all very much indeed. You have been very patient. Your evidence is absolutely fundamental to the remit of our Committee. I'm sorry if we have overrun a bit, but it was well worth it from my point of view and I am sure the Committee share the same view. Thank you very much indeed.