

Joint Committee on the National Security Strategy

Oral evidence: Defending democracy

Monday 18 March 2024

4.20 pm

[Watch the meeting](#)

Members present: Dame Margaret Beckett MP (Chair); Sarah Atherton MP; Lord Browne of Ladyton; Lord Butler of Brockwell; Liam Byrne MP; Baroness Crawley; Baroness Fall; Richard Graham MP; Sir Jeremy Quin MP; Lord Robathan; Lord Sarfraz; Lord Snape; Viscount Stansgate; Bob Stewart MP.

Science, Innovation and Technology Committee member present: Greg Clark MP.

Evidence Session No. 1

Heard in Public

Questions 1 - 43

Witnesses

[I:](#) Professor Rory Cormac, Professor of International Relations, University of Nottingham; Pamela San Martín, Member of Oversight Board, Meta.

[II:](#) Dr Mhairi Aitken, Ethics Fellow, Public Policy Programme, Alan Turing Institute; Martin Wolf CBE, Chief Economics Commentator, *Financial Times*; Jessica Zucker, Director of Online Safety Policy, Ofcom.

[III:](#) Louise Edwards, Director of Regulation and Digital Transformation, Electoral Commission; Vijay Rangarajan, Chief Executive, Electoral Commission.

Examination of witnesses

Professor Rory Cormac and Pamela San Martin.

Q1 **Baroness Crawley:** Good afternoon, everyone. This is the first oral evidence session of the committee's new defending democracy inquiry. The first panel will look at the evolving risks to democracy, including from foreign interference, and how these risks can be addressed. The second panel will consider the role of emerging technologies and what role the media and regulators play in countering challenges such as disinformation. Today's final panel will focus on risks to the election

process and the Electoral Commission's work to ensure the UK's electoral integrity. Please can I ask the witnesses to the first panel to introduce themselves?

Professor Rory Cormac: Good afternoon. Thank you for having me. It is a privilege to be here. I am professor of international relations at the University of Nottingham.

Baroness Crawley: You are very welcome indeed, Professor Cormac. With us virtually is Pamela San Martín, who is a member of the oversight board for Meta. You are welcome to our committee this afternoon.

Pamela San Martín: Thank you. I am very honoured to be here and with Professor Cormac. I am in fact part of the oversight board that was created by Meta and, prior to that, I was part of the Mexican electoral management body. I will just tell the committee that my native language is Spanish so, if I stutter a bit in English, please excuse me beforehand.

Q2 **Baroness Crawley:** Yes, of course. Your English is fantastic. Perhaps I can kick off, then. What do you both see as the greatest risk to the UK's democracy today?

Professor Rory Cormac: The greatest threat to democracy today comes to our elections. It is right that we are focusing on elections in this election year, but the bigger threat is not necessarily changing the outcome of an election in a tangible way towards a particular party. For me, the bigger threat is the wider, more insidious impact on the perceived legitimacy of those elections and the trust people have in the outcome of those elections.

To me, that is a bigger threat than focusing on, say, regime change or covert sponsorship of a change in the outcome, because the threat is chronic. It is disruptive, it is subversive and it feeds on our own internal divisions. Foreign interference is not separate from internal activity. Hostile foreign states feed and exploit our internal divisions and weaknesses. They do not create these divisions. They spot them, they exploit them, they polarise and they try to crack them open as far as possible.

The threat is this general erosion of trust, sowing confusion, undermining our trust in our democratic institutions, exploiting our own internal weaknesses and turning them against us.

Q3 **The Chair:** How have these threats to UK democracy evolved since the 2019 election?

Professor Rory Cormac: In some ways, I hope we are seeing an improvement. On the one hand there is, we like to think, less populism and toxicity around now, compared to 2019. We also have more legislation in place. That is an important part, but only—we will come to this later, I assume—one part of the defence against this type of thing. On the other hand, we see the rise of AI, which we will talk about later, and the rise of deepfakes on a mass scale that we did not see in 2019. We would be naive to assume that populism and post-truth politics are

behind us. I hope we are making steps in the right direction, but we all know how general election campaigns can be.

On a final note, there are potentially more actors willing to try to influence these elections than before, based on open material. We all know the major players, but we see from the United States, for example, that there is quite a long list targeting the US. We are not the same, by any stretch of the imagination, but there could be more actors involved.

Pamela San Martín: I completely agree with Professor Cormac. When we think of threats to electoral or democratic processes in the digital age, our first impulse is to focus on social media, AI-generated threats such as the high speed and high volume by which disinformation can spread, malicious and manipulated media, co-ordinated campaigns aimed at disrupting democratic processes. These threats are there. There is no doubt. They create enormous challenges to electoral processes around the world, and the UK is no exception.

These will probably evolve at a very fast pace, but I agree with Professor Cormac in that we have to take a step back and see other risks and challenges that are very relevant. One, as he said, is trust in democratic processes. The second is the broader issue of questioning and challenges to democracy and democratic ideals worldwide.

It is important to acknowledge that trust is central to elections. It is one of the main elements to preserve in electoral processes and it is built over time, but that can never be taken for granted. Everybody involved—electoral authorities, Governments, political parties, candidates, even social media companies—needs to safeguard and preserve trust actively at all times. This applies not only to the objective elements surrounding trust, the objective institutional design, the objective rules, the objective practices but to the public perception of trust. That is exactly why disinformation campaigns can affect the integrity of electoral processes so much.

On the second part, more broadly, it is important that we recognise that, throughout the world, even in countries that have the most consolidated democracies, democracy and the democratic ideals are being put into question. They are being challenged in different ways and forms. This risk cannot be overstated. It has proven to threaten even the most consolidated democracies.

Why is it so important to acknowledge this? When we seek to protect and defend democracy, it is fundamental that the answers or solutions that are proposed do not in themselves undermine the problem they seek to solve. What I am trying to say is that, in democracy, ends do not justify the means. The preservation of democracy is an end that has to be aspired to, but it must also be done through democratic means. The protection of democratic freedoms cannot be at the expense of those same freedoms, and the fear of erosion of democracy has taken many countries in a different direction than that.

Q4 Lord Robathan: Professor Cormac, I was very interested in your point about undermining faith and trust in the democratic process, which is a very good point. I want to pick you up on the toxicity and populism in 2019 that you referred to. Could you give us an example of that and how you think that whatever that was will not be present in the next general election, which is presumably coming later this year?

Professor Rory Cormac: We are in a better position now than we were in 2019.

Lord Robathan: In what way is it better?

Professor Rory Cormac: It is better in terms of the suitability of the two main candidates for Prime Minister. I hope we will see less engagement in the dubious post-truth politics that we saw in the run-up to the 2019 general election. People generally are more aware now of some of the challenges. People are more aware of the risks. Once we start to lose trust in the system more widely, once we start to generate perceptions that people are lying and not everything is free and fair, it is very difficult to get that trust back.

We have seen a shift. We are having discussions now about this and that is really important for raising public awareness about the threats and the risks that we are facing in a way we did not in 2019. The Intelligence and Security Committee's Russia report, for example, raised awareness of these risks and allowed us to have these debates in an open, honest and constructive manner.

That is really important, because as soon as we do not have these debates in an open, honest and constructive manner that can be exploited. It can be manipulated and we can be encouraged to turn in on ourselves. That is what hostile foreign actors want. They want us chasing each other. They want us chasing ghosts and turning in on ourselves. That is the risk.

Q5 Bob Stewart: Good afternoon to both of you. Thanks for coming. I get your point about the biggest threat being the macro point, the erosion of trust in the process. My questions are about how. You have mentioned AI, support for toxic groups—if it is acceptable to use the word “toxic”—and smear campaigns, money being sent to people and disinformation. How do they do it? You have given some idea.

Professor Rory Cormac: It is all of the above. There are three ways to influence an election and to try to undermine trust. The first way is through information operations: disinformation, amplifying misinformation and all this sort of thing. It can be done on a mass scale to generate confusion and exploit divisions, but it is very difficult to measure the impact of influence operations on a mass scale because, as I said earlier, foreign states do not create some of this stuff. They amplify it. That is the first way.

The second way to influence an election is political influence activity, such as exploiting loopholes in electoral funding laws, for example. I hope

some of that has been cleared up with the foreign influence registration scheme. This is slightly more targeted or focused than, say, information operations, but it is also difficult to measure impact.

The third way of doing it is what we call foreign interference, which involves meddling more directly with voter mechanisms, whether that is cyberattacks on electoral registration databases or hacking polling booths. Fortunately, here in the UK, it is more difficult to hack pencils and paper systems. That is a good thing in relation to foreign interference in that way.

Those are the three broad ways of doing it. Most scholars agree that the third way, the direct way, is the most difficult to do but, if you can do it, it has the most tangible and measurable effects.

Q6 **Bob Stewart:** Ms San Martín, fundamentally, where the heck do these threats come from? Is it Russia, Iran, China? Where do they come from? Who has such an interest in our democracy that they are prepared to put a lot of effort into it?

Pamela San Martín: Co-ordinated action that seeks to disrupt democratic processes or to create an atmosphere of distrust in electoral processes and democracy in itself can come from different places. It can come from within a country or from abroad. It creates enormous risks, threats and challenges for the preservation of democracy, and it has to be addressed. It cannot always be identified exactly where the threats are coming from, but the actions that they support, the impacts that they have, can be addressed throughout electoral processes.

On the oversight board that I am part of, we are convinced that social media companies must play their part in this. Many of the problems that we are living with now are not new, and companies have to learn lessons from past experience and take responsible steps to address this. For example, almost two years to the day of the storming of the US Capitol, Meta and other social media platforms were again abused by co-ordinated campaigns that ended up in an attack on federal buildings in Brazil. Seeing that, and seeing that lessons from past experiences were not learned, the oversight board pushed Meta to develop and publish election integrity metrics that should show us the steps that the company has taken and whether its efforts are working.

In November, the company announced how it would handle major elections and that one of its focuses would be fighting misinformation and preventing electoral interference. We would expect these issues to be part of those election integrity metrics. It also has been recommended that the company carry out due diligence in reviewing its design and policy choices—for example, its newsfeed, recommendation algorithms and other design features that can amplify this harmful misinformation and enable the platforms to be abused.

I will build on what Professor Cormac said. Importantly, protecting democracy and election integrity is not a one-way street. Addressing

these challenges cannot be limited to identifying and countering the actions of malicious actors. We also have to acknowledge that those actors exploit pre-existing societal and democratic fissures. They need to be addressed through democratic means, in order to give no space to malicious actors who seek to intervene or interfere in electoral processes.

One example is closing the loopholes in campaign finance regulations that allow them to intervene. It also has to do with investment in media literacy to strengthen fact-checking networks and work with platforms to guarantee that they enforce their rules adequately and can provide reliable information on issues that could seed mistrust.

Bob Stewart: I should have remembered internal attacks, too. You are right to correct me on that. Professor Cormac, as this is about foreign interference, what foreign origins of interference would you be prepared to name publicly?

Professor Rory Cormac: With the caveat, of course, that I am not privy to any classified or sensitive information, we have heard extensively from the Intelligence and Security Committee that Russia is likely to try to influence the election. The recent American intelligence assessment report on its 2024 election has named China and Iran. They will have a different relationship with us than they do with America, but clearly they are countries that should at the very least be on our radar.

Bob Stewart: Thank you. I am on the ISC, so I can confirm that.

Q7 **Sarah Atherton:** Professor, you will probably know that last December the National Cyber Security Centre—this is on open-source information—intercepted Star Blizzard, an organisation associated with Russia's Federal Security Service, which launched a cyberattack on high-target individuals. That is basically everyone in this room. How can we protect ourselves?

Professor Rory Cormac: On an individual level, the NCSC has done a good job of trying to build awareness and the robustness of our personal and business-level ability to spot warning signs, phishing attacks and that kind of thing. There has been a lot of public awareness and training. Again, it is media literacy. In this sense, it is not traditional media. It is how we engage with sources, from emails to whatever sites it may be.

We cannot just put the onus too much on individuals, because a collective, whole-of-society response is needed. There are lots of things we can do. For example, on one level, I am very much in favour of disruptive, intelligence-led offensive cyber efforts, where they are proportionate and properly overseen, to try to disrupt hostile state activity in terms of cyberattacks or to get to the root of disinformation efforts through bot farms, troll farms or whatever.

There is a role for intelligence-led disruption, alongside individual literacy and some of the legislation that we have seen over the last year or so. It is that combination of factors. We are not going to get out of this by devolving all responsibility to individuals, we are not going to legislate our

way out of this, and we are not going to cyber our way out of this. It takes a collective response from all these different pillars working together. It will be a long-term thing. We are in for a long game here.

Q8 Lord Butler of Brockwell: Professor Cormac, you have said that more research is needed. What are the main gaps that you see in our knowledge and how can they be filled?

Professor Rory Cormac: A big gap is in how we judge the impact and success of disinformation and online influence operations. Quite often, the research talks about how many clicks or likes, or whatever, a particular tweet generated. That is measuring outputs rather than outcomes. It does not measure what behavioural change those likes or tweets led to. It was for ever thus. Back during the Cold War, they measured impact based on how many newspapers they managed to get a particular article into, but that did not tell anybody what changed as a consequence.

First, measuring outcomes rather than outputs is very important. Secondly, we have an overreliance on metrics, again, to count the outputs, and more research is needed on more psychological or narrative-based approaches to how and why this works, rather than what seems like an easier option of metrics.

Thirdly, we need more research on how we reach intended audiences when we are countering this type of activity. It seems to me that we focus a lot on fact checking and exposing, which is a good thing. We should be fact checking and exposing, but it is not a silver bullet. So many of the target audiences who are most receptive to some of this material will see the fact checking and ignore it. They will see it as authored by a Government and think, "I don't trust that Government", or they will see it as authored by Meta or Facebook and think, "They're all in line with the deep state trying to promote a particular agenda".

First, we need to think very carefully about how, when and why we expose and fact check, rather than seeing it as the end goal in itself. Secondly, we need more research on more creative ways of reaching certain target audiences, to be as credible as possible and to encourage that behaviour change that I outlined earlier.

Lord Butler of Brockwell: Ms San Martín, do you have anything to add?

Pamela San Martín: I completely agree. What has proved to be more useful is when, in elections in other countries, the authorities have been able to communicate more directly with people and find a way to counter disinformation through more adequate means. Usually, when you have a disinformation message, it is quick, it is catchy and anybody can read it. When you have a fact check or a counter-message, it is robust, carefully crafted and precise, but it does not have the same impact as the disinformation message itself. That also needs to be looked into when thinking of these measures.

There is also the impact that media literacy can have on fighting disinformation. Counter-disinformation mechanisms will never be as fast as disinformation spreading or as co-ordinated campaigns aimed at disrupting democratic processes. If people are able, from the outset, to understand or identify whether what they are reading is likely to be a manipulated message, that will go a long way to achieving the objective. The exercise done in Finland, for example, is very interesting to look at.

Q9 Baroness Fall: Much has been made already of this being a year of elections. There are something like 70. We have already had a few, including a not very democratic one this weekend. Do you think that this year of elections will encourage more foreign interference?

Professor Rory Cormac: Yes, I do, simply by virtue of the fact that there are more opportunities to engage in this kind of thing, more countries and more targets. We will see an increase in the number of attempts. Of course, countries lack the capacity to interfere in too many elections at the same time. What I imagine would happen would be copycat-type things, learning from each other, not necessarily trying to change the outcome of individual elections but taking the whole thing together and trying to undermine trust in democracy more widely, across all 70-odd elections. That is what I would be looking out for.

Q10 Baroness Fall: Pamela San Martín, I want to add something to my question to you. There is some possibility of the USA and the UK having elections within a week of each other. Do you see a heightened threat there?

Pamela San Martín: There is no predetermined answer to this question. In my experience, it can go both ways. The sheer number of electoral processes, or having two very important electoral processes occurring at the same time, can have two different effects: it can hinder the actions of those who seek to undermine democratic processes, or it can become an umbrella that impedes more detailed monitoring of the different electoral processes by social media platforms, by the international community, to raise awareness with regards to what is happening in different democratic processes.

With close to 80 elections occurring this year, it needs to be taken into account that the first electoral processes that are held, especially in more democratic countries, can serve as a learning experience for those that will occur later. That can be a learning experience in attacking electoral integrity but also in protecting democracy. These examples can strengthen democratic ideals and trust in democracies and democratic processes or be a disruptive element that affects credibility of democratic processes.

All these elections occurring at the same time have outcomes unknown to this moment, but we should plan for the fact that there could be disruptive outcomes.

Q11 Baroness Fall: In this particular election, we have a background of war in the Middle East and war in Ukraine. The difference of who wins could

impact how those go afterwards. For example, it is alleged that President Trump could consider taking funding away from Ukraine. Do you think that adds to the likelihood that we could see quite a lot of foreign interference in the election, especially from Russia? Professor Cormac, could you give us your views on that?

Professor Rory Cormac: Yes, I do. Any of these contentious issues will invite foreign interference, to interfere in a way that suits that particular party's foreign policy or, equally likely, to interfere just to carry on sowing divisions and polarisation and making life as difficult as possible for those defending against it and those trying to ensure a free and fair election.

With those examples, we will see an interplay between foreign influence operations and more internal, domestic actors, where it is very difficult to draw a fine line. There are people domestically, wittingly or unwittingly, amplifying foreign policy lines being fed by certain states that might not have that country's best interests at heart. It is quite important to try to break down that foreign and domestic division and to look at how the two work together, particularly when countering disinformation.

If a country has a mandate to counter foreign disinformation but not to counter domestic disinformation because of free speech issues, how we grapple with the interplay between the two is really important. The Middle East is highlighting that right now.

Baroness Crawley: We have just had an election in Portugal, and I wondered whether either of you had monitored that in any way or looked at it, as far as foreign interference or disinformation are concerned.

Professor Rory Cormac: I have not, no.

The Chair: It looks as if neither of you have.

Pamela San Martín: No, sorry.

Q12 **Lord Snape:** In your assessment, Professor Cormac, how does the National Security Act 2023 address the evolving state threats to UK democracy? There has also been some criticism of the Act as too narrow. Concentrating purely on national security means that other aspects of Britain's democracy could be threatened.

Professor Rory Cormac: That is fair. It is a good thing. It gives extra tools to counter or disrupt the sharp end of foreign interference, making it easier, I hope, to catch false declarations of money, for example, or people operating directly on behalf of a foreign state. At the sharp, direct end, it gives us more tools.

It does not look at that greyer, more insidious area—where arguably a bigger threat comes from—where the agent is not directed by a foreign power. I am talking about the foreign influence registration scheme here. What about people who are operating in the interests of, but are not directed by, a foreign power? What about the use of opaque shell

companies to channel this material? In that sense, it is narrow. That is not to say that what it is doing is not a good thing, but there are lots of loopholes that can be exploited. It misses this greyer area.

Hostile foreign states have traditionally exploited that grey area between legitimate and illegitimate, and exploited the various loopholes. I fear that this could happen here too. The Act, for me, takes an assumption that democratic resilience is generally healthy in the UK. The security side of things is making life difficult at the sharp end, but—as we have alluded to already—there are other issues, maybe below the level of national security, which can be exploited. The Act does not necessarily cover these.

It is not that it should. You cannot legislate for all of this stuff, which is why I will go back to the initial point about resolving some of our internal issues and focusing on media literacy among everybody, from young people all the way through. We cannot legislate our way out of this but, as legislation goes, it is a step forward and it has given us tools that we have not had in the past.

- Q13 **Viscount Stansgate:** You have just said—and in fact have repeated twice now—that you cannot legislate your way out of it. Nevertheless, we have a National Security Act 2023. Can I ask you about one aspect of that? That is the foreign influence registration scheme, to which you have made a brief allusion already. How is it intended, in your view, to strengthen the resilience of the UK?

Professor Rory Cormac: It is intended to strengthen the resilience of the UK by making life more difficult for hostile foreign actors. It gives us a neat piece of legislation to prosecute where appropriate and it does so without having to air what might be classified material and open that whole can of worms around how we deal with covert influence cases, so I think it will disrupt. It will make life more difficult for those wishing to do us harm.

Viscount Stansgate: You mentioned covert influence. What about covert money? How far do you think the Act of 2023 addresses the challenge of the possibility of foreign money being used to influence elections?

Professor Rory Cormac: It deals with the really sharp end. It gives a way to catch false declarations, but it does not go far enough in the broader sense. You will know there were various discussions in the run-up to the Act and there are clearly, as I see it, loopholes that can be exploited by hostile foreign powers in relation to companies and unincorporated associations, where there is potential to bypass the Act.

It comes back to a point I mentioned earlier. The Act seems to be based on the assumption that we do not have all these loopholes and grey areas, so we needed an Act that would capture the sharp end. It still has all this wider political grey area, which can be exploited, and it could have gone further.

Q14 **Viscount Stansgate:** The Act does not make any distinction between foreign and friendly countries. How much of a potential problem is that?

Professor Rory Cormac: I can see where the Act was coming from on this, because there is always a risk in having lists of friendly and unfriendly countries. I can see how that would become problematic quite quickly. On balance, it was a sensible approach, but there is a risk of increasing burden and red tape on everybody else in order to satisfy the requirements of an Act in which genuinely hostile actors may find loopholes anyway. As is often the unintended consequence of legislation, this increases the burden on everyone else trying to deal with it.

I can see how they have tried to get around that with the two-tier approach, but increased administrative burden is a risk and I will be watching very closely to see how that plays out on the ground.

Q15 **Liam Byrne:** Just to round out the point on financing, Professor Cormac, at the moment it is perfectly possible for a significant amount of money earned in a foreign country to come into the bank account of a UK citizen and then go straight into the coffers of a political party. Surely that is one of the biggest loopholes that we should be trying to fix.

Professor Rory Cormac: Yes, it is. There are numerous loopholes that can be exploited. That is a very good example. We should be doing more. The question for me is whether that becomes a national security issue or an issue of domestic politics, standards of public life or whatever it may be. That gets to the point of how we need a whole-of-government, whole-of-society approach to dealing with this. There is a risk. When we siphon some of this stuff off into different sectors, it can risk being overlooked.

Liam Byrne: It may have made more sense for us to legislate so that only money that has been earned in the UK can go into a British political party, for example.

Professor Rory Cormac: Yes.

Q16 **Liam Byrne:** Pamela, you have said a couple of times that the role of social media companies is, in your words, to safeguard trust. You said earlier that social media companies need to do their part in supporting the democratic process. Can you just lay out a little more simply for us what you see as social media companies' responsibilities when it comes to safeguarding democratic integrity and elections?

Pamela San Martín: Social media companies have the responsibility of enforcing their own policies, their own values, in a fair and transparent way, in which users are treated equally. The positive sides of social media platforms, which enable people to access information and to participate in electoral processes, must be safeguarded but, at the same time, there are risks of the platforms being misused to undermine democratic processes, exclude certain voices and enable certain criminal actors to participate in electoral processes.

For example, Meta has tons of risk evaluation and mitigation measures in place that it can apply to elections. In order for it to complete that role and act according to its international human rights responsibilities, it has to put all these tools and these measures into play during elections.

Liam Byrne: In a world where, as we have heard from Professor Cormac, you have bad actors trying to sow aggression and division on two sides of an argument, would it not be helpful if we had a definition of hate speech in this country, so that we could take out more easily that kind of divisive behaviour? Take, as an example, Germany's NetzDG law.

Pamela San Martín: The problem of having a government-sponsored definition that will limit freedom of speech is that they can be overly enforced. They will be overly enforced by social media.

Liam Byrne: Is that what has happened in Germany?

Pamela San Martín: That is what has happened with all the laws that have been approved that have very strict obligations for social media platforms to remove content. Given the volume of content that moves through social media platforms, those platforms have overly removed content so as not to be non-compliant with state legislation.

It also gives an example to countries that may not be democratic countries, and that may have other intentions when regulating speech online, to start overly restricting freedom of expression. We have to be aware of that, because we have been building the guarantees to ensure freedom of expression for more than 200 years and we cannot lose sight of those guarantees.

Liam Byrne: That is true, and you have talked about the need for transparency as one of the remedies for this, but we do not have transparency into Meta's algorithms, for example, which promote a particular kind of content to the top of people's feeds.

Pamela San Martín: We do not. That is one of the things that we do not have much transparency on. The board has recommended that, at least, Meta should evaluate and carry out due diligence to determine how its designed algorithms impact how harmful disinformation is amplified on its platform. What is it doing to address these issues so that its platform is not misused? That should be expected from all social media platforms. We should be able to know how their design decisions impact conversations, especially during elections.

Liam Byrne: But we do not have it yet.

Pamela San Martín: No, we do not.

Liam Byrne: Should we legislate for it?

Pamela San Martín: Legislation on transparency can be very positive.

Q17 **Richard Graham:** On the same issue, Pamela San Martín, any of us with

social media accounts can spot the large numbers of obvious bots that are there commenting. In August last year, the *Guardian* reported that Meta had closed 9,000 Facebook and Instagram accounts linked to Chinese spamouflage—in other words, foreign influence campaigning. Is there not already enough analysis going on of the number of fake accounts? Building on what Liam Byrne was suggesting, do you think we can make it harder for accounts to be opened, so that those that are opened have gone through some form of certification beforehand?

Pamela San Martín: There is one thing that we cannot lose sight of. It is not only malicious actors who use social media. People get informed through social media. People communicate through social media. People access information that is very relevant to democratic processes through social media. People organise politically, legitimately, through social media. If you start putting these sorts of measures into play, it will not be the malicious actors who are impacted. They will find loopholes to go around that. You will impact legitimate speech that needs to be preserved online.

Anonymity, for example, is one of the core elements of social media infrastructure, which enables it to be a platform where people can communicate. Safeguards have to be put in place to avoid misuse of platforms. Trends and co-ordinated campaigns have to be part of those safeguards that are put in place. We would expect that to be part of Meta's election integrity efforts, for example, but it is not through putting bigger blocks into opening social media accounts.

Richard Graham: I understand the argument about the balance and the need for democratic intercourse and so on. None the less, a small cyber company in my constituency was employed by Meta and Google during the recent Indian elections and was taking down literally—it told me—millions of Facebook posts every day. Do we have the balance right?

Pamela San Martín: I believe that we have to insist on policies being enforced adequately, being enforced according to the policies that have been put in place, and being enforced equitably, so that users are treated fairly in the enforcement of social media platforms' policies. Are we there right now? No. Will we ever have the exact, precise balance? No. Given the sheer number and volume, there will always be mistakes, but we have to push social media platforms to make sure that those mistakes are less common and do not impact elections or the political speech that is so relevant to democracy around the world.

Richard Graham: Professor Rory Cormac, what are your thoughts on this issue? If millions of Facebook posts have to be taken down during an election in India, will we face the same thing in America and possibly here? Is there not something wrong with a system where that volume of fake news has to be monitored and, inevitably, quite a lot gets through?

Professor Rory Cormac: Social media companies could and should be doing a lot more to take this stuff down quickly and to share their material with non-state actors, with academia and with Governments, but

I worry that an overly legislative approach to this would, again, just create the loopholes that genuinely hostile states would exploit and everyone else would be encumbered by.

Finally, when it comes to disinformation, Governments should not be arbiters of what is true and what is not. There is very rarely a clear line. It is good to have things such as Meta's oversight board taking an independent approach to this, because as soon as Governments get involved, it becomes politicised. People instantly start to accuse Governments of being partisan or toeing a particular line, which can end up doing more harm than good.

The Chair: Thank you, both of you, for coming to give evidence to the committee. We appreciate it.

Examination of witnesses

Dr Mhairi Aitken, Jessica Zucker and Martin Wolf.

The Chair: Good afternoon. All three of you are very welcome. I hope it will not inconvenience you too much if we move on fairly speedily to the questions.

Q18 **Greg Clark:** Thank you, witnesses, for coming. Can I start by asking Mr Wolf to give us his perspective on the threats to our democracy, particularly to UK elections, from technologies and, in particular, AI?

Martin Wolf: That is a fairly scary question to start off with. How many hours do you have? This is one of the areas in which I feel least confident, in the sense that I understand some of the issues involved in what is going on now, but I am looking forward to hearing the other witnesses on what this means.

Let us get to first principles. Democracy is fundamentally based on public discussion and debate, and the possession of reliable information, which people trust is reliable and on the basis of which they can discuss with confidence with one another. Those are pretty close to the necessary conditions for democracy to run. I have been thinking about how democracy evolved, and it is pretty clear that the emergence of the press played a pretty important part in that. I would not say that all parts of the press have achieved that to an equal degree at all times, but who was doing it and what they were saying was transparent. In the 20th century, public service broadcasting played a pretty big part in our democracy.

If we are in an environment in which there is a risk of widespread and sophisticated fakes, in which many people believe, because they look very plausible, and in which tainted information of all kinds is spread, the consequence of which is more likely to be simply pervasive distrust than that everybody will trust any particular one of these, that is bound to or

at least highly likely to make the functioning of a democracy substantially more difficult and democratic institutions less stable.

Q19 Greg Clark: You are a journalist of great distinction and a columnist of influence. How does it feel for you in this important election year in this country? You contribute analysis to help people make these decisions. Does it feel more difficult for you this year to have the influence that you have had in previous years as a result of some of the development of these technologies?

Martin Wolf: I have two answers to that, which is probably not very satisfactory. First, I try very hard never to think—I think I am 100% successful—about the influence I might have in anything that I write. I always start from the assumption that it is zero, which is probably a good bet, first, because one does not know at all and, secondly, because it is grotesquely self-important. I really do not know whether this affects anything.

Secondly, I am privileged, given that I write about economics and finance, to be writing for the organ that I write for. It has a pretty small readership, which I tend to think has two important characteristics. It is very well informed, and it is paying rather a lot of money to read the *Financial Times* because it thinks it is getting a certain value.

I do not think that, with our readers, the environment more broadly is particularly affected. You just have to think who they are. Most of them are people involved in business and finance, or things close to that, and the reliability of information is more or less life and death for them. They have to have something that they trust, and that is why they read the *FT*. I am not saying that we are the only ones, but that is why they read it. This is not necessarily true of everybody in the marketplace, and our readership is pretty tiny compared to that of the electorate as a whole.

Greg Clark: Ms Zucker, you are the online safety policy director for Ofcom—in other words, the communications regulator. You have responsibilities for regulation as well as the education of the public, if I can call it that. What is liable to be the most influential area? Is it to educate the public to spot disinformation and manipulation, or can the path of regulation offer some dependable protections?

Jessica Zucker: Unfortunately, there is no silver bullet solution here, which is why we are taking a multifaceted approach to how we look at these threats. The Online Safety Act empowers Ofcom to hold platforms to account for the first time and to ensure that they put in process systems that effectively prevent the spread of illegal harm. In this case, that constitutes foreign interference.

There are a number of ways in which we will be able to hold these platforms to account to ensure that they do something about this. In our set of proposals for illegal harms, which we published at the end of last year, we have set out some of the ways that we suggest that platforms do this. They include having sufficiently staffed content moderation

teams, and having really robust governance processes to make sure that seniors at organisations are aware of the risks.

We are asking platforms to do risk assessments, to look at the risk of foreign interference on their platforms and to take appropriate measures to address those risks. Some of the biggest platforms that we call categorised services—a subset of the 100,000 companies that we will regulate—will be subject to additional duties such as transparency reporting, where we will be able to ask them to publish information about these kinds of risks and what they are doing to address them.

We will also be putting in place something called the terms of service duty. Many of the biggest platforms have policies on foreign interference, inauthentic behaviour, and mis and disinformation. We will be empowered as the regulator to hold them to account to enforce those rules if they say that they have them.

Media literacy, of course, is another area that we are investing quite a lot in. We have had considerable powers for the last several years. One of the ways that we are thinking about media literacy is to help users on these online services find and identify misinformation when they come across it. We have been running campaigns and are partnering with external organisations to do just that.

Greg Clark: You speak mostly in the future tense. The Online Safety Act is now law. Do you feel that Ofcom has put in place for this important electoral year the necessary protections that the law requires and empowers you to put in place?

Jessica Zucker: The Online Safety Act received Royal Assent at the very end of last year. As soon as that happened, we published our first set of proposals on illegal harms. Parliament asked us to prioritise the most severe harms first, so we started with the first phase of our regulation, which is on preventing the spread of illegal content, foreign interference being one example, alongside child sexual abuse material, grooming, fraud and violent hate speech.

The second part of our regulatory implementation that Parliament asked us to prioritise is protecting children against potentially harmful content. The last phase will be the additional set of duties that the biggest and highest-reach services will have to put in place.

We are taking a phased approach. The way that Ofcom approaches regulation is through an evidence-based process. We take our time to ensure that we have a certain threshold of evidence that we can then turn into impact assessments and propose measures that platforms take. Where we are now in the process, we published our first set of proposals at the end of last year. We closed our consultation about a month ago. We are reviewing that information and will update our codes of practice and guidance documents likely by the end of this year.

Greg Clark: By the end of the year is too late for the election.

Jessica Zucker: It potentially is. We do not know when the election is, but we are in the process now of assessing the data that we got from this consultation period. We do have to do a consultation, which is the first step of this regulatory process.

Greg Clark: The Prime Minister has helpfully indicated that the election will be in the second half of this year. Can you act on that and bring forward your steps so that they are in place in time for the election?

Jessica Zucker: We are moving as quickly as possible. As soon as the Bill received Royal Assent, we published our first set of proposals right out the gate. It is a process that requires us to look at evidence. Proportionality is important. We are requiring services to do things that are quite novel, so we are following a set of processes to make sure that we hold them to the highest standards and have evidence to go back to.

Q20 Lord Butler of Brockwell: Continuing on the theme of UK politics, we have already seen some notorious deepfake videos and audio involving, for example, President Macron, Joe Biden, Imran Khan, Sadiq Khan back here in Britain, and even Keir Starmer. How confident are you, if I may address this to Jessica Zucker, that Ofcom will be able to detect these fake videos and audio that may appear in the lead-up to our general election and put a stop to them?

Jessica Zucker: One of the good things about the Online Safety Act is that it is tech neutral, which means that it can withstand the test of time. If somebody creates a deepfake video, for example, using the new kinds of generative AI content, and posts it on one of the services that we regulate, which is either a search or user-to-user service, that content is regulated by the Online Safety Act.

As I mentioned before, that empowers Ofcom to hold the platforms to account when it comes to the spread of illegal content. I mentioned a couple. You mentioned certain types of deepfake videos. Some of the risks that we anticipate are deepfakes with non-consensual sharing of sexual imagery, pornographic material, or material that harasses. These are the types of things that will be covered by the Online Safety Act.

I should also say that we have seen other, less sophisticated forms of disinformation in the last few years that remain a persistent threat. These are so-called cheap fakes or less sophisticated types of disinformation where there is light editing. It might be splicing or cropping a video, or changing an image in a way that might mislead. These are things that we are also seeing and which present challenges for the platforms.

Lord Butler of Brockwell: Is it a challenge that you will be able to meet before the date of the general election?

Jessica Zucker: As I mentioned before, we anticipate our powers coming into full force at the end of this year, once we have finalised our illegal harms consultation. That said, we do have our powers on media literacy, which we are actively using. One of the ways that we are planning to do so is running a campaign that targets new voters aged 18

to 24 to help them spot disinformation and identify different types of critical thinking skills that might be needed in order to spot that.

Lord Butler of Brockwell: It is not your fault, but it seems to me that we are a bit late to the game in this respect.

The Chair: I believe, Dr Aitken, that you are going to show the committee a relevant image.

Dr Mhairi Aitken: Yes, I have an image here. It is an AI-generated image.

An image described as deepfake was shown.

This is an image of the aftermath of an earthquake and tsunami. It is the Cascadia earthquake in Oregon of 2001, which you would probably not have heard of. You may have heard of it last year, though, because these photos were created in 2023 using Midjourney and shared on a Reddit group that shares AI-generated content. It shows a fairly convincing image of the aftermath of a natural disaster. Many AI-generated images such as these are being shared online of politically relevant or sensitive events, as well as of natural disasters such as this.

When you first look at it, it is fairly convincing, but there are telltale signs when you look more closely, and we have the advantage of seeing it quite large here. First, the text on the sign at the bottom left of the screen looks from a distance as though it probably has words or text. If you look closely, you will see that the letters are not identifiable or distinguishable. It is garbled. This is a common sign of an AI-generated image. Even the most sophisticated AI image generators struggle with producing legible, coherent text, so that is one sign to look for.

Another sign in this image is in details such as traffic lights. If we were to expand on those, you would see that they are a bit fuzzy around the edges. They are not fully formed. These are things that you probably would not notice if it was a small image that you are looking at on your phone and that had been shared on social media. When we look at it large, we can see those details.

There is police tape running along the side. If you look at the far left of the image, you can see that it fades away. It looks as though it must be secured very tightly, but we can see that it fades off into the distance. These are some of the sorts of details and signs to look for.

There are other things that you might look for in a potentially AI-generated image, such as whether shadows fall in the right place. Look at the background of an image. The foreground might be quite detailed, crisp and clear, whereas the background may be a bit more impressionistic or less detailed.

Taking it further, if it is an image reporting an event on a particular day in a particular place, you can check the weather conditions to see whether they are as they should be. If there are people in the image, a

fairly well-known one now is counting the number of fingers—AI image generators have a long history of struggling with fingers—or the number of teeth in a mouth. Details such as the texture of the hair or the skin can be giveaway signs.

It is important to note that these technologies are becoming more sophisticated and convincing all the time. There are still signs that we can look for, but it is becoming much more difficult to accurately and consistently identify AI-generated outputs.

These are images that we can see on a large screen, but, for the most part, these are probably low-resolution images that are shared on social media. People are mostly scrolling past images on a small screen on a phone.

It is important to emphasise that the responsibility here should not be on individual users or individual members of the public to scrutinise all images or all online content. Instead, we need to think much more carefully about the responsibilities of platforms on which these images or potentially AI-generated content are shared, and how we can ensure transparency around the ways that AI-generated content might be being created and shared.

These are some tips or things to look for in AI-generated images, but it is important to emphasise that this should not all be about putting the responsibility or the expectation on members of the public to scrutinise all content.

Q21 Lord Butler of Brockwell: This question is again to Ofcom. Will you have an expert panel who are watching this sort of thing, or will you be relying on the platforms to do it?

Jessica Zucker: The Online Safety Act is not a content takedown regime, so it does not mean that people at Ofcom will be looking at individual pieces of content or at individual complaints. Instead, the Online Safety Act is designed to look at online harms at scale by looking at the systems and the processes that platforms have to deal with these kinds of issues.

We will be putting together an advisory committee on disinformation probably towards the end of the year. That committee will consist of experts on disinformation as well as UK-specific disinformation issues. That committee will be tasked with advising Ofcom on our duties that are relevant to mis and disinformation, including how we use our transparency and media literacy powers, as well as the other relevant duties that I mentioned relating to foreign interference and applying terms of service effectively.

Q22 Viscount Stansgate: How quickly did you realise that it was a fake?

Dr Mhairi Aitken: I have to confess that, in this instance, this example was shared on a Reddit page where people were sharing AI-generated

images, so I knew it to be fake when I came to it. Knowing that it is fake, you scrutinise these images more.

Viscount Stansgate: Take another example that you have not seen before. You realise that it is a fake. How quickly can you act to take it down?

Dr Mhairi Aitken: It is a matter of ensuring transparency. This is not necessarily about taking images down but about having the transparency to clarify that these are AI-generated images. If they are AI-generated images that are being spread for malicious purposes, to cause harm or to humiliate or incriminate, that is clearly a case for taking those images down.

Viscount Stansgate: Suppose that, in the middle of an election, an image like this, of damage or bombing, suddenly appears in Britain. Some group claims or does not claim responsibility for it. It could cause a great deal of interest and alarm. If you realise that it is fake, how quickly can you take action to tell everybody that it is fake?

Dr Mhairi Aitken: This is a real challenge. At the moment, these images could be flagged or reported. When they are politically sensitive, they may be taken down more swiftly.

Viscount Stansgate: You do not know how quickly you could do it. You mentioned an advisory group that will be set up towards the end of the year. As my colleague over here has said, that will be too late for the likely date of an election. We might go through an election period where something like this happens every day, for all we know.

Q23 **Greg Clark:** May I just clarify one of the answers that Ms Zucker just gave? You mentioned the creation of a disinformation and misinformation advisory committee. That is, in fact, required under Section 152 of the Act. In October last year, in answer to a question from Lord Clement-Jones, the Minister, Lord Camrose, said that it was “the role of Ofcom to create it” and that he would “liaise with it to make sure that that is speeded up”. I take from your answer that the group has not been created yet.

Jessica Zucker: No, and that is because Parliament asked us to prioritise the most severe harms first. It has asked us specifically to prioritise illegal harms, which we have done, and, following that, protecting children against potentially harmful content.

Greg Clark: When Lord Camrose said that he undertook to liaise with Ofcom to make sure that it is speeded up, are you aware of the conversation that the Minister had with your organisation?

Jessica Zucker: It is possible that that has happened. I do not recall directly, but I can tell you that we are prioritising this alongside the rest of our statutory duties. Unlike the duties that we have on illegal harms and protection of children, we have statutory deadlines that we need to make. We plan on setting this up as quickly as possible. It takes time to

find the right people and to run an open and fair process, and we are doing that.

Like I said, we are not ignoring the fact that this is an issue. We have media literacy powers in place and are thinking about a number of ways in which we can start bringing information out into the public, through commissioning research, publishing discussion papers and running media literacy campaigns that highlight the risk of disinformation.

Greg Clark: Nearly six months ago, the Minister told Parliament that he would make sure that it is speeded up. Has it been?

Jessica Zucker: I should also note that the Online Safety Act does not specifically identify mis or disinformation as a harm that platforms need to take into account when they are putting these protections in place. The primary way in which the disinformation risks are addressed under the Online Safety Act is through the terms of service duty that I mentioned and through the transparency reporting, as well as a number of other foreign interference provisions. That is where we are focusing our efforts.

Greg Clark: That is despite what the Minister says.

Jessica Zucker: I do not think that those things are mutually exclusive.

Q24 **Lord Browne of Ladyton:** The questions that I was intending to ask have already been engaged with, but I am not entirely sure that they have been answered. I suspect that our witnesses do not think that there are easy answers to any of them.

This new technology and these fakes are moving at a pace that is very difficult to keep up with. Dr Aitken, you said that they are getting better all the time. How confident is Ofcom that broadcasters will be able to detect and stop the publication of these if they improve and are much better than that one was? There were not that many mistakes in it, to be honest.

It seems to me that we will get to the point where we are asking the platforms to take this responsibility primarily, which I can understand, but this will just be too good and it will fake them too. It cannot be that far away. We are constantly catching up with this technology, and we cannot help that, but it is pretty obvious that that is what we will be doing very shortly.

Jessica Zucker: You are right that the technology is evolving rapidly, as are the risks around it and the way that people use these technologies and online services. As I mentioned, the Online Safety Act is technology neutral, which means that it is about the harms that are created rather than the types of technology used to address those. We are doing a lot of research as Ofcom, as are organisations such as the Alan Turing Institute, which puts tools out there for the public, for users and for platforms to use to better detect it.

At Ofcom, the kinds of research that we are doing to understand the risk and detection of deepfakes include inscription—using watermarks as a

way of labelling AI-generated content so that it can later be identified as such. We are looking into ways of preventing the malicious use of deepfake technology, such as looking at the kinds of datasets used for training generative AI models, as well as novel detection methods that can indicate when something has been generated by AI.

These are things that Ofcom is looking into and researching. As we have more information, working with organisations such as the Alan Turing Institute, we will be able to iterate on our codes of practices that set out the proposals that platforms need to put in place to address these kinds of risks.

Lord Browne of Ladyton: It seems that we, as a country, are on the route to an AI regulation policy that regulates at the point of use, not at the point of development. Eighty per cent of deepfakes, for example, are created for misogynistic or revenge porn purposes. Should the reality of this technology not cause us to rethink the point at which we regulate it? Some of these technologies should be regulated or banned at the point of development, as opposed to the point of use, because they have no positive use. They are designed to fake people. The answer is in what they call them: they are fakes. Every other fake I know about is illegal. It will be almost impossible to regulate this if we regulate it only at the point of use.

Dr Mhairi Aitken: That is a really interesting point. When we look at the regulatory applications across the AI life cycle, there are decisions made at all stages from the early design of AI models, through the development of those models, and into how those are deployed and used in context. There are important decisions made at all those stages, so we need to think very carefully about the expectations around ethical and responsible practice through all those stages.

In the case of generative AI, these are largely developed as general-purpose AI models that are not designed to be used for a particular function but can be further developed or deployed in different contexts and for a variety of purposes. That raises the challenge of the extent to which the potential harms or risks are fully anticipated in the design and development of models that might be deployed for uses or in contexts that were not fully anticipated in the earlier stages. It certainly presents particular risks, and we should explore how to ensure that there are responsible and ethical approaches throughout that life cycle and not just at the point where those technologies are deployed and are being used.

At the moment in the UK, the regulatory approach to AI is looking at how the uses of AI fit within the remits of existing regulators in the wide variety of contexts and purposes for which they are being used. That reflects the fact that AI is being used across a wide range of sectors and across all industries. Currently, regulatory bodies across all sectors are needing to grapple with the challenges of regulating the uses of AI.

That points to the need to make sure that there is access to state-of-the-art expertise in AI so that we can not only react to what is currently

happening or what we are currently seeing, but anticipate how these technologies might develop and be used in a year or two. That points to the importance of having access to state-of-the-art expertise in cutting edge AI technologies.

- Q25 **Viscount Stansgate:** In the middle of an election, if an image occurs or a deep fake is produced, will Ofcom be ready for the questions it will face as to whether or how you could tell that something is fake or real? Major national broadcasters might turn to Ofcom and say, "You have a role in this". Are you prepared for what may be coming in the middle of what could be a very heated election campaign?

Jessica Zucker: As I mentioned, the Online Safety Act is not a content takedown regime, so my team will not be looking at individual instances of such content-making decisions. Instead, we are looking at the systems and the processes. I mentioned in relation to the timing that the duties on online services will likely go into effect at the end of the year. That is also to say that platforms can very well get on with implementing the Act, and there is nothing preventing them from doing that. We have already seen some platforms taking active steps to apply the duties that we have set forth in our draft proposals, which is a positive sign.

We also have our media literacy powers. I mentioned that we are thinking about a campaign to target new voters on how to spot mis and disinformation. Working with organisations like Dr Aitken's institute would help us to empower the public to better spot and identify these types of things.

- Q26 **The Chair:** Mr Wolf, I gather that a phrase that is used is the "liar's dividend". There is so much false information circulating that we reach a stage where people find it impossible to recognise what is true and what is not. How much does that worry you? How likely do you think that is?

Martin Wolf: It worries me a great deal. I do not know whether we are there yet. I think not. There are clearly very important areas of decision-making where the degree of scepticism about what people are being told, partly because of the way they are interacting with others on platforms and the sort of evidence they are given, is socially completely horrifying.

One of the most interesting areas to me, because it is so surprising to me, is the transformation of the level of scepticism about vaccines. If I had been asked 25 years ago whether what we have seen in many very sophisticated countries was possible, I would have said that it is inconceivable, because every damn fool knows that vaccines work, but that is no longer true. That is a pretty fundamental medical achievement. It is one of the great revolutions, which started here, and there is now immense scepticism about it.

These are pretty primitive systems for spreading misinformation. There are possibilities of numerous other fakes generating social panics of various kinds, which we have seen in the past, where popular hysteria is encouraged and you end up with massacres. This is part of human

history. Out-of-control information and disinformation of this kind can be socially harmful on a catastrophic level.

The big question I have is partly addressed in my book and is not new. I have already mentioned examples such as the St Bartholomew's Day massacre. The most important mass disinformation case in European history was in the 1930s, which led to the Holocaust, so it is not new. I cannot make up my mind as to whether the technology itself is so transformative that it will become a completely unmanageable problem. Having heard the discussion already, I am not more optimistic than I was when I came into the room.

As a complete ignoramus, I was just reading about the possibility of having systems that could convert stories into completely plausible feature film-length things. If the technologies in question were also given the information required to replicate living individuals pretty well perfectly, the potential of fakes of this kind could be extraordinary. We are clearly at a very early stage of new technologies with potentially extraordinarily far-reaching consequences. Given what has already happened in the last few years in the areas I have mentioned, with reactions of various kinds in many ways, it is very disturbing and I do not know how easy it will be to regulate it, although I am very pleased that somebody is trying.

The Chair: I take your point entirely. One of the things that has been important to me for all my life is to understand that there is a difference between evidence and opinion.

Martin Wolf: There is clearly a difference conceptually. The question is whether we will be able to differentiate in this context.

The Chair: One of the things that I have learned is that it already seems that many people cannot.

Q27 **Liam Byrne:** Jessica, I am not quite sure how you can judge the integrity of the processes that you said you are policing without getting involved in examining the content. When we began thinking about the Online Safety Bill, we had in mind the safety at work legislation from the early 1970s. We would not really judge whether health and safety at work processes were working without having one eye on the accidents or fatalities that might have been going on in a workplace. Are you seriously telling us that you are not going to be looking at online content when you are making judgments about whether processes are working?

Jessica Zucker: My job is to implement the Act as it is currently in legislative form. The Act does not say that Ofcom should be looking at content and making decisions about that. We have put out a set of proposals that explain the specific steps that platforms need to take to address the degrees of different harms. Those steps are meant to be quite specific. We can look, for example, at whether a platform has terms of service. Those are the rules that platforms need to put in place that say, "This is what is allowed and not allowed on a platform".

Liam Byrne: Can you withstand the pressure of, say, during a general election campaign, people inundating you with examples of content, to which you reply, "I'm really sorry, but we don't look at content. We just check that the processes are in order"?

Jessica Zucker: Unlike the regulations that we have in broadcasting, Ofcom does not have a complaint centre that is meant to look at individual pieces of content. That is clearly laid out in the Act. Again, my job as online safety regulator is to implement the Online Safety Act.

Liam Byrne: So there may be a shortcoming in the law.

Jessica Zucker: It is not for me to say. That is a matter for government and Parliament to take up. My job is to implement the Act.

Q28 **Liam Byrne:** How big is the resource that you have available to check the safety of these platforms? How much resource do you have to check that the Online Safety Act is being effectively implemented?

Jessica Zucker: The UK Government appointed us online safety regulator in 2020. Since then, we have been staffing up and trying to find the right expertise to make sure that we can do this job. At the end of last year, we had close to 350 people across the organisation. This consists of a mix of expertise. We have online safety experts with expertise in individual harm areas that are covered by the Act. We have experts in child sexual abuse, in foreign interference and in grooming, for example. We also have data scientists and economists. We have researchers and lawyers. We have regulatory delivery specialists. Cumulatively, we work together to implement this.

Liam Byrne: Are you satisfied that you now have the capability to implement the Act effectively?

Jessica Zucker: It is not for me to say. We have a huge team that is working together.

Liam Byrne: Are you not the director of online safety policy at Ofcom?

Jessica Zucker: That is correct. We are in the early stages of implementing the Act.

Liam Byrne: So it clearly is for you to say whether you have the capability in place.

Jessica Zucker: We are in the early stages of implementing the Act right now. Like I said, we have been focusing on building up the capabilities in the group and on going through each phase of the regulation. At the end of the implementation phase, the Secretary of State will be required to look at the efficacy of the Online Safety Act. That will be a good time for Ofcom to then input into a formal process as to how the regulation is working in practice.

Liam Byrne: So we have to wait and see, in effect.

Jessica Zucker: Like I said before, we are in the early stages of implementation. We are following the direction of Parliament to implement for the most severe harms first. We have published our package of proposals on those illegal harms. We are now going through the evidence and finalising those proposals, which, again, will be published at the end of this year.

Q29 **Liam Byrne:** We have heard that transparency around algorithms, for example, will be really important, because we know that platforms such as Facebook can promote divisive content to people. Do you think that that transparency is important effectively to police these platforms?

Jessica Zucker: Transparency will be one of the most powerful tools that we have under the Online Safety Act. Certain types of platforms that we consider categorised, which I can explain, will have to publish information that we have asked them to. Ofcom will then look at all the platform's transparency reports and publish our own analysis of whether we think that things are going well, and of good and bad practice.

Q30 **Liam Byrne:** The UK Government have just intervened in the debate about the Digital Markets, Competition and Consumers Bill to prohibit foreign state ownership of a UK newspaper, because they are worried about a different kind of algorithm called editorialising and do not want foreign state ownership control of something such as a newspaper with a digital platform attached. They were inspired to act by the takeover bid for the *Daily Telegraph*, but TikTok has twice the news share of the *Daily Telegraph*. If the UK Government are acting to legislate to stop state ownership of the *Daily Telegraph*, should we be following the example of the US House of Representatives and legislate to ensure that ByteDance divests itself of TikTok here in the UK?

Jessica Zucker: The scope of the laws is not a matter for Ofcom but for government and Parliament to decide. These are separate issues. We are talking about state ownership, which is a slightly different issue from user safety.

Liam Byrne: Mr Wolf, what do you think?

Martin Wolf: I have no views on ByteDance—in other words, whether TikTok is a threat—although I have read a lot about it. As a more general point that I have thought a bit about, if we want to change the behaviour of companies, leaving aside banning them, there have to be severe penalties for disseminating false and dangerous content. In other words, as you would expect, they should have the responsibilities of publishers, because that is what they are.

Since I am an economist, I also happen to believe that incentives change behaviour. It seems to me pretty clear—I read quite a bit about this in doing my book—that a number of quite important platforms have not cared very much about the consequences because it is very profitable for them not to do so. Incentives matter, so in future legislation we should take some of the lessons that we have learned from banking regulation.

- Q31 **Baroness Fall:** Mr Wolf, you are a well-known and highly respected commentator. The traditional media has more trust in a way, but fewer people using it, especially among the young. Coming into this election year, is there a role for more trusted newspapers such as the one you work for to play in the election and, if so, what sort? "Full Fact" came to the BBC, which was relatively new for previous elections. Is there something that newspapers can do to earn the trust of the electorate?

Martin Wolf: Our view is that elections are part of what we do. We cover them in great detail and depth, with the resources that we have at our disposal, which are not infinite, and we do so for our subscribers.

This is where it gets difficult. One way that one could imagine, without committing our organisation, is to change paywall rules during an election campaign, but that is not very likely. As I have discussed before, the really interesting point is that the economics of information demands that it be free in some sense because it is a public good, but the economics of businesses generating information demands that it not be free because it is a private good. By putting vast resources into coverage of the election, as we certainly will, we are no more able than any other organisation to give it away for free.

That is true even with the BBC, which is paid for, although at the margin it is free. We cannot have a model quite like that. Every media organisation has to think about how it operates in the context of an event as significant as an election. Basically, it is part of the news, and that is what we do.

Finally, and crucially, we cannot make people read what they do not want to read. I am afraid that our articles are quite long, detailed and full of facts, and we will never be able to compete with a number of other organs in the number of people who read them. That is just something that we have to accept. It is part of a free society.

- Q32 **Baroness Fall:** Mr Wolf, you are saying that, coming into an election period, newspapers with their high paywalls should be thinking about that in terms of people reading from the same place and having, in a sense, a truth or reality that they share.

That brings me to a point for Dr Aitken. On social media, it is the opposite problem. Masses of information is disseminated where we cannot necessarily see it and what it is saying to different people. In what sense can we work with social media companies to see a bit more of what they are up to and to get best practice coming into the election?

Dr Mhairi Aitken: It is really important to recognise that where people are getting their information from and how they access the news is changing, certainly across different demographics and age groups. Social media sites such as TikTok and Instagram are increasingly a source of information about the world. Particularly for young people, that is where they seek and access the news.

It is really important that we pay close attention to how that information is being filtered, shaped, prioritised and served to different users. It is very often prioritised through algorithms that create profiles of individual users in order to serve them content that is most likely to keep them engaged on those sites, not necessarily with the incentive of that being the most accurate information. That is a real problem, and we definitely need to demand more transparency and accountability in the ways in which these algorithms are being used and the impact they are having on how people access information about the world.

There are real risks to that increasing personalisation of information, especially in the way information is being served through prioritising information that will keep people engaged. A lot of research has previously pointed to that often being the information that is most likely to shock or the most polarising information, leading people to increasingly consume information in echo chambers that reinforce existing world views, prejudices or political ideologies. That is a concern.

With traditional media, where people were consuming the same media, they were exposed to and challenged to encounter different points of view and perspectives. There is a risk that, as information about the world is increasingly consumed in these more isolated and personalised echo chambers, we do not have the same exposure to alternative perspectives and views, and the opportunity to challenge them, which is of fundamental importance in a democracy. It is really important that we pay attention to the ways in which the information is being consumed across different platforms. This is an area of importance.

Q33 Richard Graham: Martin Wolf, can I come back to you as one of, I suspect, several fans of your column in the *FT*? Forgive me for not yet having read your book *The Crisis of Democratic Capitalism*.

Martin Wolf: You are in good company.

Richard Graham: In that book, did you tackle the issue raised by some of the written evidence that we received before this session, which was about what the authors called democratic autonomy? Their argument was broadly that the less citizens know about their political options, the less we achieve democratic autonomy.

They went on to suggest that disinformation muddies trust, citing, for example, Russia's information on Hillary Clinton, leading citizens into thinking that she had more character shortfalls than her opponent. One of their solutions to this was to give a dollop more money to the BBC to expand what it is doing, both domestically and abroad, to try to improve voters' trust in the information they are getting. Is that a good solution?

Martin Wolf: As I said at the very beginning in response to Mr Clark's question, trust in information, and ideally shared trust, where people would agree, as the Chair suggested, on what the facts are—there is the famous remark of Daniel Patrick Moynihan on that—is essential for any functioning political process.

As we have also heard, the algorithms that work for the platforms are very clearly not designed to produce information that deserves to be trusted. Although it might, by accident, deserve to be trusted, it spreads what spreads. It is designed to function like a virus that does what viruses do, which, to me, is simply terrifying. That is why I talk about the platform responsibilities.

How do you respond to that? There are basically only two ways I can think of. One is to change the incentives for the platforms, which is very complicated, and the other is to strengthen such public service institutions as we have, which may be old-fashioned and will certainly not have the effectiveness that they had 40 or 50 years ago when they were a monopoly.

I would argue that countries that are lucky enough to have inherited from the past public service organisations that are reasonably trustworthy, such as the BBC—that view is now quite controversial, but I continue to hold it—should do everything they can to maintain that model. I am influenced in that to a significant degree by looking pretty carefully at the literature and the evidence on what has happened to the US in the last four decades, and it is not a very pretty picture.

Richard Graham: So your answer, effectively, is yes.

Martin Wolf: I apologise. It was a lengthy answer to give a rationale for the answer being yes, without thinking that it is a magic cure in any way, because it is not.

Richard Graham: Dr Mhairi Aitken, are there other solutions that a country like ours should be looking at to increase trust in information?

Dr Mhairi Aitken: We have seen developments such as content credentials, for example, and providing more information about the veracity of images. The BBC recently launched content credentials, where it provides evidence about what it has done to check the veracity of an image and to identify that it has not been AI-generated, and provides information about the source of an image, how it might have been edited, and metadata in content that is shared.

There are technical solutions like that that need to be there. They are an important component of how information and content are shared through the media. Importantly, public understanding and transparency are needed with these technical tools. As I said before, the emphasis should not be on expecting members of the public to scrutinise all content, but they should have access to a reliable and trusted source of information from a reliable, trustworthy body that provides those assurances about that content and provides a place and tools to verify online content.

There is a lot of interest in the development of technical AI detection tools and the use of watermarks to identify AI-generated content. Those could be digital watermarks, which would not be visible in the images or

the videos, but through the use of AI detection tools it would be possible to detect those watermarks in AI-generated outputs.

This is a really important area and we need much more research here to advance these techniques. At the moment, AI detection tools often have quite low levels of accuracy, so we need to be very cautious about how we use them and the extent to which we rely on them. Systems such as digital watermarking can work well where people are in compliance, but if there is a malicious actor seeking to deliberately spread disinformation or create fake content, these devices can currently be circumvented.

There are technical solutions, but there are also important social or political solutions for how we maintain trust in institutions of the media, as well as political institutions. That is not purely a technical challenge; it is a challenge to do with the relationships that members of the public have with the media as well as with political institutions.

Q34 Lord Browne of Ladyton: On this subject, the real power of the algorithm is its ability to understand and anticipate or reinforce our patterns of behaviour from the data that we create, which is how they sell things to us. That is what these people do through misinformation. So is it not the case in that world that the people who are intent on harm create these same patterns? Is it not possible for algorithms to detect the people who are there for malicious purposes? Do they not leave a pattern of behaviour that would direct us to where they are operating and that would therefore justify us stopping them operating in the system at all?

Dr Mhairi Aitken: This is an area where we have to be really cautious. As I said, tools that are designed to detect AI-generated content currently do not have sufficiently high levels of accuracy to be relied on. In education settings, there has been a lot of interest in developing AI detection tools to detect potentially AI-generated coursework. These have consistently been found to have low levels of accuracy and, importantly, to have disproportionately false positives for students whose first language is not English.

This is an example of where using or relying on detection tools might inadvertently create inequitable outcomes or lead to biased outcomes that, if we use them in social media platforms, could lead to censorship of voices, experiences or political ideologies that are disproportionately falsely identified through the use of these tools. We need to be really careful about relying on these detection tools. Currently, they are not accurate enough to be relied upon.

Lord Browne of Ladyton: I heard you say that before, and I accept that. Despite the fact that we are both Scottish and speak the same English, I may not have made my point properly to you, so let me have another go at this. We are all influenced by this world of algorithms. We all have a news app on our phones, which serves us the news that we want to hear about the football team that we follow or whatever. These algorithms know our patterns of behaviour and feed the information to us.

I understand that, in the European Union's attempt to regulate this behaviour, it is on to this subject, but bad operators create patterns of behaviour as well. Is there not some way in which we can use the algorithm's ability to do this to help us identify where they are operating, so that we can home in on and stop them early in the process as opposed to trying to catch up when they have done the damage and gone?

Dr Mhairi Aitken: There is lots of interest in how we might develop AI tools in combating online harms or in identifying malicious actors or harmful outcomes. We need to be cautious. This is an important area where there needs to be a lot more research to look at how we might develop tools for these kinds of purposes or for tackling malicious or harmful actions. We need to be cautious about relying on AI tools to address problems created by the use of AI tools. Technical tools will provide some of the solutions, but this also needs to be tackled through thinking about social, ethical and responsible innovation practices. There is a danger of relying purely on technical tools to address the risks created.

Q35 **Viscount Stansgate:** You mentioned watermarks. If you print fake money, it is against the law. The Royal Mint is constantly designing new types of note to make them more difficult to fake and to build trust in people who use them that they are real. Do you have some hope that there could be a watermark process for digital imagery—either single images or videos? If so, can it come quickly enough?

Dr Mhairi Aitken: There is a lot of interest in how digital watermarks might be developed. One of the challenges is that these watermarks might be embedded in outputs produced by a particular model, which can then be detected by software that has been developed to detect AI-generated content produced by that particular model.

One of the shortcomings of this is that, if you wanted to scrutinise whether a particular image might have been AI-generated, you might need to use lots of different AI detection software to see whether it has been produced by each of the various models that that detection software is able to detect the outputs from. We need to think about how we could have a joined-up, coherent approach that can reliably identify AI-generated outputs across the full range of models.

There are further risks or limitations around this. Malicious actors can fairly easily circumvent compliance with digital watermarking currently, particularly if these were developed by use of an open-source model. Even if that model was developed to have a digital watermark produced on the outputs, if we are using an open-source model it could easily circumvent the embedding of that watermark into those outputs by altering some lines of the code.

This is an area where it is important that we have more research and develop these techniques swiftly and rapidly. This is urgent. These techniques cannot be relied on as things currently are.

The Chair: Thank you. I am afraid that we set ourselves quite a

challenge today to try to get through three panels as smoothly and speedily as we can, and it is a challenge that we have failed. In fairness to those who are providing the answers in the third panel, we must thank the three of you very much indeed for your contribution.

Examination of witnesses

Louise Edwards and Vijay Rangarajan.

Q36 **Viscount Stansgate:** My question is very simple. What are the key threats facing democracy, and how is the Electoral Commission seeking to defend democracy in everything you do?

Vijay Rangarajan: It is a pleasure to be here. This is week three for me, so forgive me if I do not know all the answers, but I have Louise Edwards with me as director for regulation, who has huge experience in the Electoral Commission. I was going to break down the threats into five areas. A couple were not covered earlier in the session, I think, so I will give a little response on those. Some of them are the issues you have been working through in the previous two panels.

I will start from the position that trust in our electoral system is still remarkably high. According to our data, and we do regular surveys, three-quarters of people polled are confident that elections are well run in the UK, and 80% are satisfied with the process of voting. That is obviously the end stage of an election; we have much less information on the previous elements of trust in information and trust in the media.

There is one large set of issues that is a real threat to that trust and to democracy, which is physical threats to candidates. We have all seen a lot of that over the last few years. I will go into a little more detail on that because the previous panels did not. We monitor this very closely. We survey all candidates. We will try to step that up this year. At the moment, between a third and a half of candidates who responded to our survey said that they had a problem with abuse, intimidation or harassment. It is particularly acute, as many of you will know, for women candidates, ethnic minorities, those on the Front Benches and in some parts of Northern Ireland.

This is a real problem. It is making some candidates withdraw, maybe self-censor and maybe not stand. That seems like a real threat to our democracy. What are we doing about that? We certainly do not want to see, as it were, the victims changing their behaviour. We do not want to see self-censorship or candidates not standing because they are worried about the threats to themselves or their families, either on or offline. We are working very closely with the police, clearly. You will know that we propose, and it is now entering into force and is in Parliament next week, that security expenditure for candidates should not count towards campaign finance. That is in order that candidates can have what security expenditure they need without jeopardising the really tough campaign finance limits that you all know we have on candidates.

We have given candidates guidance on potential criminal offences so they can draw the attention of the police and others to those offences. From last November, anyone found guilty of these offences can be barred from standing for office as well as the criminal sanctions. That is partly to dissuade some of the actors, some campaigners, who are also guilty of some of the abuse. There is a large set of areas related to physical abuse, which is also sometimes online. Sometimes the two are intimately interlinked, with harassment and abuse coming online followed up by physical intimidation.

I will move more quickly through the others. There is a significant threat in mis and disinformation. You have already more than touched on this. Social media companies, we know, have a lot of responsibility here. We are working closely with Meta, Google, X, Snap and TikTok on what they can do, with varying degrees of success.

There is no law governing campaign material itself, so let me go into a little more detail on what we would like campaigners to do and what we hope voters will be able to do. One is voters looking at material with a sceptical eye. I think they are broadly used to that. There have been hundreds of years of material that was questionably truthful or accurate coming up in election campaigns. It is part of the process. I think they will look at it sceptically, but that needs to be reinforced even further.

On campaigners themselves, coming back to a point raised in the earlier panel, where there have been some quite remarkable deepfakes of very senior politicians, such as the audio recording we all know about, we think that the campaigners themselves reacted very well when it was noted it was a deepfake. Sometimes we will be able to attribute this, but I do not have a high expectation that it will be possible, technologically or quickly enough, to credibly attribute a deepfake by some third party. The campaigners themselves saying, "This is a deepfake", and others not playing along with that will be a very important part of the behaviour.

We proposed a while ago, and Louise may want to say much more on this, the system of imprints for campaign material. It is very interesting to hear your previous panellists talk about watermarks for AI. That would be an interesting thing to say, "This is AI generated". That is not necessarily a bad thing, by the way. We are focused on AI deepfakes being used to mislead voters, and that is the particular threat that we see. We are seeing examples in other parts of the world of AI being used to engage voters truthfully and helpfully. Maybe we could go into those if you would find that useful.

There are, as I said, the physical threats, the AI threats and information. There is a big cyber threat, which I can go through quite quickly. We, the Electoral Commission, had a major attack, as you know, in 2022. Political parties have been targeted as well, as have MPs. I think that cyber threat will grow. We are working very closely with the National Cyber Security Centre to try to make sure that all these elements of what is a form of critical national infrastructure are indeed protected to the greatest extent possible.

Finally, foreign direct interference, which was raised by Professor Cormac earlier, is always possible. We have seen plenty of examples of it around the world. The point that he and Pamela San Martín made, that we can learn a lot from other elections around the world in this particularly election-rich year, is important. We are talking to other electoral commissions in other countries. The European Union has European parliamentary elections coming up now. There is the US election campaign running. For our closest neighbours, there is an Irish election. There are many of these that we will be watching closely to make sure that, where we see a threat or a new technique, we can at least look at this and be a little more prepared for when it happens to us for the first time.

The final area I wanted to mention on this list of threats is finance and donations from abroad. You have touched on some of the issues there. We think there are ways to tighten up the financing rules. Mr Byrne mentioned at least one of them. Professor Cormac mentioned, I think, unincorporated associations and making sure that companies cannot spend more money on donations than they make in the UK.

Those are the main threats that we see. Set against that, we have a system that has a high degree of resilience. It is paper-based. It is not as susceptible, as has been said, to cyberattacks. It can be re-counted. I am sure that we will be re-counting some. It is, I hope, one that will maintain—that is certainly the Electoral Commission’s aim—high trust by voters and campaigners at what is a crucial democratic moment.

Q37 Chair: You made a number of recommendations to the Government in 2018 and 2021 to increase transparency of online campaigning, which has been referred to a number of times in the evidence today. How many of those recommendations have been implemented?

Louise Edwards: A fair number have, and I will go through some of them, which I am quite pleased to see. Having been one of the people who worked very hard on that report, it is fantastic that this number of years later we are still talking about it and some of them have come into effect.

The first one to mention is digital imprints, that bit of text that you see that tells you whose campaign material it is, or indeed that bit of audio if it is audio, or something on a video. The commission has been calling for that since 2003, and it eventually came into law at the back end of last year. We are very pleased to see that. We will be looking very closely at how that is complied with in the elections coming this year. I am very happy to talk a little more about that if you would like me to.

We also made a series of recommendations that were aimed at how social media companies can be more transparent about the political advertising that they see on their platforms. A lot of that was about trying to encourage the use of what are called ad libraries, the libraries that a number of them publish that set out what political adverts have been paid for on their platforms. Any member of the public can go in, do

some searching and find out what sort of money has been spent by particular political actors.

One area there that we are pushing for more on is to encourage the social media companies to bring the definitions they use for things such as political advertising into line with the legal definitions, because at the moment it is a bit of a Venn diagram. It is not entirely 100% that something that is regulated under law will definitely be in the ad library and vice versa. That is an area we are still pushing on.

I would like to mention a couple, which I know Vijay has just touched on, that have not yet come into force and which we hope will in future. They are very much on the finance side. One is about encouraging political parties to have risk-based due diligence processes. There are literally tens of millions of pounds going through our political system every year. In 2023, £93 million worth of donations were reported to us. There is more than £1 billion worth of donations on our website and there are no due diligence provisions in law for the parties that are receiving them.

The second thing is company donations and making sure that we are closing any loopholes and putting additional safeguards in the system in relation to money coming in from outside the UK that is not lawfully coming into the system.

Chair: One thing that strikes me, and I have not heard anybody comment on it, is that we have something in the order of 2 million extra overseas voters about to come into the system. It seems to me that, apart from their impact electorally, they are a potential source of donations. This may be one reason why the change was made. I am not aware of any regulation that deals with that area at all.

Louise Edwards: They will come into the franchise, which obviously is a matter for Parliament to decide. Having been enfranchised and entitled to be on the electoral roll, these individuals will also be entitled to make donations to political parties. That is why it has always been quite important, when talking about foreign money coming into the UK political system, to talk about lawful foreign money and unlawful foreign money. Since the regime was established, overseas electors have been able to donate money to political parties.

There is a regime and a structure in place around donations coming into the UK's political system. Very broadly, it is about putting a sort of wrapper around the UK of what is called permissibility—permissible individuals or permissible organisations. There are legal obligations on political parties to take steps to identify who the donor is and to satisfy themselves that the donor is permissible. All those newly enfranchised voters will come under that same regime, so there will still be those responsibilities on political parties. As I have mentioned, we think that those responsibilities should be enhanced by the introduction of risk-based due diligence.

Q38 **Chair:** Can I go back to the question of disinformation and ask what is, I

am afraid, a rather sweeping question? What does it seem to you is the risk in a general election if false information remains unchallenged?

Louise Edwards: One risk that we have already mentioned is around people wanting to get stuck into the election in the first place. One fundamental building block of our democracy is people who are willing to campaign and stand as candidates—political parties, non-party campaigners and candidates. If false information, or the fear of risk of false information, puts people off becoming candidates, campaigning or volunteering for their local political party, that is a huge, significant and very unfortunate impact.

There is another category of information that could be wrong, and that is information about the electoral processes. In fact, in the local elections last year, we saw leaflets being distributed that had the wrong forms of voter ID on them, meaning that somebody relying on those leaflets may have turned up to the polling station and not have been able to vote. Fortunately in this country there is a trusted source of information about electoral processes, which is us. Therefore, if there are questions about false information about electoral processes, we will be able to say whether it is right or wrong and to mobilise our social media channels and partners, including media partners, to make sure that it is very clear that that piece of disinformation about the electoral process is wrong.

Moving on to more campaign-based disinformation or the deepfakes that have been discussed here a number of times, we are in a similar situation to some of the people who have spoken to you before. There is no legal framework for the content of campaign material distributed by parties or campaigners, so we are in the space of encouraging voters to look at the situation critically and to try to understand what they can do to check the veracity of information that they see.

We work with a lot of other regulators, including Ofcom, to do this and to signpost people to where they can find information about how to verify whether something is truthful. We look to campaigners to call it out themselves and the resilience of political parties and campaigners themselves to try to work in this space. There is not a law that we can enforce here, so these are the mechanisms that we use.

Chair: It has struck me, listening to this, that people make the general observation about commercial transactions that if it seems too good to be true, it probably is. Maybe this is an attitude that we should encourage more generally.

Q39 **Liam Byrne:** I think that about £1.2 billion in donations are now recorded in the Electoral Commission database. Am I right in saying that a significant fraction of that is from quite a small number of individuals?

Louise Edwards: I honestly would not know. I would have to interrogate the database to find out.

Liam Byrne: You would be there for a long time, because the information recorded in the database is not standardised by name, for

example. An individual may be recorded by one name with one donation, but they could also be listed by four or five other names—for example, with the use of initials—so it is really difficult. I say that having done it myself. A significant fraction, maybe 25%, of electoral donations are from a very small number of people. It is still the case, is it not, that money from a foreign source can go into the bank account of a UK citizen and then go into a political party as a donation perfectly legally?

Louise Edwards: That would depend on whether there was an agency situation in the case. There is a provision called the agency law, which is where somebody acts as an agent of another person. If somebody were to say, “Hey, give me the money and I’ll give it on your behalf”, you are creating an agency situation there. That would be illegal. That would be a matter for the police to investigate.

Q40 **Liam Byrne:** Taking the example flagged by the *New York Times* in 2022 of about \$630,000 coming from Russian bank accounts into the bank account of a UK citizen and then going on to a major political party here, was there an agency problem involved in that donation?

Louise Edwards: I am aware of the donation that you are talking about. Agency provisions are provisions that can be investigated only by law enforcement, not by the Electoral Commission. However, we made inquiries at the time and had no reason to think that we needed to use our enforcement powers.

Liam Byrne: The source of some of this money was businesses in occupied Crimea.

Louise Edwards: We did not need to use our enforcement powers, so I have not investigated that matter.

Liam Byrne: But the loophole was obviously there, because the money was transferred.

Louise Edwards: Again, we did not investigate it, so I do not know the exact circumstances in that situation. You are right to point out that there are areas of electoral law of the finance provisions that can be tightened up. We have mentioned some of them before, such as the due diligence provisions in relation to how companies can make donations. We can touch on unincorporated associations as well. Those are the areas that we recommend are looked at very strongly to see where additional safeguards can be placed.

Liam Byrne: In between elections, there are not really spending limits that bite.

Louise Edwards: No, that is right. The spending limits are tied to what is called a regulated period. For a parliamentary general election, for political parties and campaigners, that is 365 days ending with polling day. We are in a regulated period now. We must be, no matter when the general election is held. For candidates it is different. There are long

campaigns and short campaigns that have different spending limits attached to them.

Liam Byrne: There is that old saying that you cannot fatten a pig on market day. For political parties, there is an incentive to spend significantly in between regulated periods. At the moment, there is no cap on that spending.

Louise Edwards: There is no cap on the spending outside regulated periods. If the spending happens before a regulated period but is used for campaigning during it, it is caught again by the law. Parliament has put spending limits in place in a period running up to a poll.

Liam Byrne: Between regulated periods, I could spend that money on social media and there could be algorithms that promote some of that social media to the top of people's feeds. At the moment, we do not have any transparency around those algorithms.

Louise Edwards: That is correct.

Liam Byrne: At the moment, nobody is checking the content of a political message. We have just heard from Ofcom that it has no powers to do so.

Louise Edwards: Parliament has not put a legal framework around that.

Liam Byrne: As we sit here today, we have also heard that there are unlikely to be any safeguards in place in relation to the creation of deepfakes until before the end of the year. Is that your understanding too?

Louise Edwards: We are not aware of any legislation going through Parliament on that at this time.

Liam Byrne: We have a situation where it is still permissible for significant amounts of money to come into the bank account of a UK citizen and then into a political party. There is no limit on how much money like that can be spent between regulated periods and there is no one checking the content that that money is spent on.

Louise Edwards: Again, with money coming in there is a provision in law. It is what is called the agency provision. It would be a matter for police to investigate if they thought that there was evidence of agency having taken place. Putting to one side an actual criminal offence being committed, you find yourself in the regime that Parliament has decided, which is that spending limits apply only for a period before a poll.

I would highlight, though, that we have one of the most transparent political finance systems in the world. Spending, when it happens in the run-up to elections, is provided to us in itemised spending returns, with tens of thousands of individual lines of spending and millions of pounds' worth of spending that all gets published on our website and is transparent for everyone to see. There are also statements of accounts

that come in every year, so you can see the income and expenditure going into political parties. Crucially, there are contact details for every political party on our register to ask questions.

Q41 Liam Byrne: We all have agents who have to sweat and fill those forms in. How many investigations or prosecutions have there been for this sin of agency?

Louise Edwards: We would not investigate or prosecute it because it is a criminal prosecution, and Parliament decided to remove our power to prosecute. I am aware of one instance of convictions in 2021. This is why, when Parliament was considering the Bill to remove our powers to prosecute criminal offences, we said that that had to go hand in hand with good discussions with the police and the Home Office about how they would ensure that the police were equipped to take up this area.

Liam Byrne: We can route significant amounts of money into the bank accounts of UK citizens from foreign nationals and that money can go on to UK political parties. You are right that there is one barrier to prevent that, which is this issue of agency, but we have had only one prosecution by the sound of it. You can spend pretty much whatever you like between regulated periods and no one will check the content that you are spending the money on. Nor can we look into the algorithms that might put that content to the top of somebody's social media feed. That is broadly accurate.

Louise Edwards: I would dispute some of the claims there, because you are talking about criminal offences that may well be committed. However, if there are gaps in the political finance framework that you are highlighting, we would be very interested to explore that and see what recommendations we could make to Parliament to try to close them.

Liam Byrne: I am struggling to see the things I have got wrong in that description. Maybe you could highlight what you think the gaps are in the electoral law that Parliament should attend to if we want to defend our democracy with some stronger defences.

Louise Edwards: We have mentioned some of them already today, and Vijay may want to come in with others. We have mentioned things around the political finance system, where we could consider enhanced due diligence for political parties. You have asked a finance question, so that is quite relevant. We have talked about company transactions coming through from outside the UK. We have touched on the concept of unincorporated associations and their ability to get donations from outside the UK and then, provided there is no agency relationship, to pass that on.

We have also touched a bit on what we think should be, and we hope are, meaningful conversations with the police, making sure that they are well equipped and well resourced to pick up these challenges, particularly when they are criminal offences only.

There are a number of other recommendations that we would encourage Parliament to look at, set out in our *Digital Campaigning* report of 2018 and other places, to make sure that we can enhance the safety and security of our electoral system. However, I come back to what Vijay said at the very start, which is that our electoral system is highly trusted. There are very high levels of confidence in the public that our electoral system is well run. That is something that we need to safeguard.

Q42 Liam Byrne: At the moment, a company headquartered and registered in Gibraltar, for example, could also make a donation to a UK citizen, who could put the money into a political campaign or indeed a political party. At the moment, the opacity of the accounting system in, say, Gibraltar makes it impossible to trace the fountainhead of that cash. Should we also tighten that up when we are thinking about the way we work with foreign countries or indeed with overseas territories?

Louise Edwards: As the director of regulation for the UK Electoral Commission, I do not think I am in a position to talk about transparency of Gibraltar or countries outside the UK.

Liam Byrne: If the money is laundered from Russian sources into a company account in, say, Gibraltar and then pushed into the bank accounts of UK citizens, that is a problem.

Louise Edwards: I feel like I might end up repeating myself, so I will let Vijay answer.

Vijay Rangarajan: One recommendation that we made that I think is germane to the challenge, which I quite understand—this was picked up in the Elections Act—was effectively to put almost a prohibition on people and organisations that are not eligible to register as a third-party campaigner, including foreign organisations, spending more than £700 on campaign activity. That falls very much in the campaign periods, but, in effect, in that entire period, which, as Louise has said, starts a year before a general election anyway, a foreign organisation transferring that money in is committing an offence, because it is effectively not allowed to be a third-party campaigner and cannot spend more than £700. That is the limit, which came down significantly. Louise might want to expand a little more on that.

One method for getting money into our system that you are describing is basically fraud by a political party accepting a donation that it knows has not come from the person who is donating. Louise explained why parties could more uniformly—some do it very well, by the way—look behind their donors and do a full due diligence on them. It is exactly to try to prevent a kind of chain reaction of someone trying to channel money into them. They do a lot, and you are aware of the kind of work that agents do for campaigners. There is a risk, particularly for the larger donations, and hence the importance of the risk-based approach looking right behind that. If they were to find a non-permitted donation, it would be an offence to accept it.

Liam Byrne: I take that point, but having tried to pursue this with the Electoral Commission in 2018, we very quickly ran into the Electoral Commission's lack of investigative capacity. We ended up having to give up, despite some pretty well-founded suspicions that significant amounts of money were in effect laundered through foreign Governments and foreign accounts into a political campaign that had a significant bearing on the course of our country's future. Unless you have not just the powers but also the investigating capacity, frankly, we are not necessarily going to have the defences that we need.

Q43 **Viscount Stansgate:** Can I ask one quick factual question? As a result of the change in the law, how many additional electors based outside the UK will be taking part in this election this year or whenever it is?

Louise Edwards: We do not know.

Vijay Ranganathan: They can still register. I do not know exactly how far before a general election they are still able to register. We know that, where they are registering, electoral registration officers, despite being very hard-pressed people, are taking a lot of trouble to check that they are eligible to register. There are lists. We were in a meeting earlier today running through some of the reasons why someone had moved away when they were two years old. They claimed they had lived in a certain area, but they could not prove it. EROs will go to a lot of trouble to try to make sure that that person can be registered if they have a reasonable claim, but they are checking every one and it is proving quite a lot of work for them.

There could be a significant number of people joining the electoral register, but until we are through the parliamentary general election we will not know exactly how many. We will be looking at some of that, and we are looking now at exactly what data is useful to do in our post-poll reporting.

Chair: Thank you for your evidence and for your patience in us overrunning.