

Digital, Culture, Media and Sport Sub-Committee on Disinformation

Oral evidence, HC 2204

Tuesday 18 June 2019

Ordered by the House of Commons to be published on 18 June 2019.

Watch the meeting

Members present: Damian Collins (Chair); Clive Efford; Julie Elliott; Julian Knight; Ian C. Lucas; Brendan O'Hara; Jo Stevens.

Questions 56 - 200

Witnesses

I: Bob Posner, Chief Executive, Electoral Commission, and Louise Edwards, Director of Regulation, Electoral Commission.

II: Sasha Havlicek, CEO, ISD Global; Chloe Colliver, Lead, Digital Research Unit, ISD Global; Philip Gradwell, Chief Economist, Chainalysis; and Tom Packalén, Chair of the Board, Utopia Analytics.

Examination of Witnesses

Witnesses: Bob Posner and Louise Edwards.

Q56 Chair: Good morning, and welcome to this evidence session of the Digital, Culture, Media and Sport Committee, Sub-Committee on Disinformation. We are delighted to welcome representatives this morning from the Electoral Commission for the first panel.

Before we start this session, I would like to make a short statement giving an update on the Select Committee's inquiry on reality television. The first oral evidence session for this inquiry will be with ITV on Tuesday next week, where we will put questions to the Chairman and Chief Executive of ITV, and also to Mr Tom McLennan, who is the Executive Director of "The Jeremy Kyle Show", and Graham Stanier, who is Director of After-Care at ITV, who is also responsible for the welfare of participants in "The Jeremy Kyle Show".

"The Jeremy Kyle Show" is an important programme that we will be looking as part of the inquiry into reality television, but we believe that Jeremy Kyle himself should be an important witness to that, as the show is based around him as the lead presenter of it. We have sent an invitation to Mr Kyle through his representatives, and we have received word back from them that he has declined to appear in front of the Committee on Tuesday next week. We believe that Mr Kyle is an important witness to the Committee in its work, and we will be pursuing this matter with Mr Kyle's representatives to see if we can find a date when he will appear, or to understand fully the reasons why he is not able to appear. We will make a further statement once those discussions have concluded.

I now turn to today's evidence session. I want to ask the Electoral Commission if, first, we could discuss their recent investigation into financial donations to the Brexit Party, particularly donations through PayPal. This is an issue that the Committee has taken an interest in, and was, indeed, part of the discussion we had at the recent international Select Committee meeting in Ottawa, where we discussed these issues with the American Federal Electoral Commission as well. We are hoping to take evidence soon from PayPal to discuss these matters too.

I put the first question to Mr Posner and Louise Edwards: do you think there is a big vulnerability now in micro-donations made through online services like PayPal being exploited as a way to bring impermissible donations into political parties?

Bob Posner: Good morning. Thank you, Chair. Online payment systems in use by political parties is with us. It is a fact of life, and it has been for some time. We issued guidance back in 2015 to political parties about the use of online systems, including PayPal. They can certainly be used effectively and properly within the law. They can be used in a way that enables checks on permissibility and parties to comply, whether those



donations are above the £500 threshold or whether they are lesser sums of money.

It is a means of payment that is with us. It is a means of smaller donations coming to political parties, which, from the point of view of participation by people in politics, elections and democracy, is a positive thing. However, certainly we agree it needs to be used properly by political parties. It is something we certainly monitor and keep an eye on.

I will pass to Louise in a moment, but the only other comment I would add is that established parties, major political parties, certainly use those systems and as far as we are aware use them broadly sensibly and properly, and we keep an eye on that. When newer parties come on to the scene, we are very vigilant with them, and that is to assist them to act properly, as it were, as well. It is something that is with us. Louise, do you want to add to that?

Louise Edwards: Yes. PayPal is a tool. Online payment providers are a tool. They have to be used properly by political parties. Political parties should be and are aware of their duties and legal responsibilities when it comes to things like recording transactions properly, checking permissibility. If they are using tools like PayPal, they need to make sure that is properly written into their procedures, staff are trained, and that they are used properly, so they can meet their legal obligations.

There are some areas where these systems could be improved. We have made recommendations in the past, for example, that would help us understand how PayPal is used more effectively, or other payment providers are used more effectively, for example, by giving us the ability to get information out of companies like PayPal without having to open a formal investigation to do so. That would very much help us with our monitoring work in this area.

One of the other recommendations that we have made is that the Government should think about anti-money-laundering legislation and whether any of those regulations should apply to political parties. At the moment they do not, and there is some fairly good, solid basics of things, like written risk assessments, written procedures and training that might be very applicable to political parties and may well help address some of the risks.

Q57 **Chair:** Yes. You say that some political parties have been using these systems for some time and have systems in place to make sure people understand what their obligations are. Is there a difference, in your view, between the way these tools are used by some parties as opposed to others? Do parties that have been using them longer, maybe more established parties, have better systems in place than newer parties do?

Bob Posner: There is no reason why a newer party should not be able to do these things properly. By definition, established parties have been around longer, so they are more experienced. However, sometimes



HOUSE OF COMMONS

newer parties include experienced people who have worked with other parties and then join them. As the regulator, we see no reason why, and we would expect all parties from the very beginning to comply with the law. That must be right.

- Q58 **Chair:** Yes. You said in your report under your press release statement on 12 June about your investigation of the Brexit Party—I would like to note for the record and for anyone following proceedings this morning that the Electoral Commission has released a fuller statement on its investigation, which has been published as a result of a FOI request by the Electoral Commission. The Committee has also received a copy of it, and there is now a copy of that available on the Select Committee website as well, for anyone who would like to read that now.

You said that as a result of your investigation you believe that the Brexit Party is open to a high risk of receiving and accepting impermissible donations. Why do you believe that?

Bob Posner: Just for clarity, and it is just language, but we do not have a formal investigation open against the Brexit Party. Our work with them currently is an assessment of the situation, assessing whether they have complied or not. It is absolutely right: we say they are at a high risk of not complying and that is why we have made a number of requirements and recommendations of them to make sure they do comply. Indeed, if they did not, we would look to more formal investigative and enforcement work.

- Q59 **Chair:** Your statement says “high and ongoing”. That would suggest that there is a risk now and that as things stand you see nothing that would suggest that risk is going to be mitigated in any way unless they change their policies and procedures.

Bob Posner: Yes, they need to take action. That is absolutely correct.

- Q60 **Chair:** Why has the high risk occurred? Does that mean that you believe there is a good chance they have already received impermissible donations because they do not have good enough systems in place to detect those donations?

Bob Posner: It is certainly the case that we are not satisfied with the systems they have in place. It is the responsibility of all political parties only to accept donations if they can reasonably satisfy themselves that they are accepting permissible money within the rules. That is very important. That underpins our whole system in the UK. It is vital to have those systems in place so they do not inadvertently or advertently fall foul of those rules. That is what they need to do.

- Q61 **Chair:** I am trying to understand what sort of systems these might be. What is it that they do not do that they should do?

Louise Edwards: The first area that we looked at is around the information that you gather when you are receiving money through PayPal or other online payment providers. One of the recommendations



HOUSE OF COMMONS

we have been making for political parties since 2015 onwards, when we first started looking at this, is things like: make sure if someone is giving you some money you get their address. Match that with the bank account that the money is coming from, for example, so that you can see that the person who is claiming to give you the money and the person who is giving you the money are the same person.

Q62 **Chair:** It might be easier to take this step by step. Are those things that, based on your assessment, the Brexit Party have not been doing?

Louise Edwards: That is right, yes.

Q63 **Chair:** They have not been collecting addresses of donors or checking whether the donor has authorisation over the bank account that has paid the money?

Louise Edwards: Not systematically. This, as I say, is why PayPal is a tool, and it has to be configured properly by the party that is using it to give that party the information that it needs. This is all about making sure that, first of all, you can identify donations, particularly if they may be split into smaller amounts. Then when you have identified a donation, make sure you know where it has come from and have some system of checking that and keeping a record, so you can keep track of any aggregations as well.

Q64 **Chair:** There the risk would be that someone may hypothetically be making many, many donations, using a different name each time, but it is all coming out of the same bank account?

Louise Edwards: Essentially, yes, or breaking a donation down into smaller amounts so that it is under the threshold of £500.

Q65 **Chair:** Yes. What about donations from overseas?

Louise Edwards: First of all, I would say that it is entirely possible that a political party could get a permissible donation from an elector who is registered overseas. It is not as straightforward as just saying, "If it comes in a different currency it must be impermissible". Essentially the same thing applies; you need to be able to check permissibility. You need to identify that a donation has been made, even if it is split into multiple, small amounts, and then you need to have sufficient information to check that against the electoral role. It is the same principle whether the money is coming in from outside or from within the UK.

Q66 **Chair:** In your view there was no effective system in place created by the Brexit Party to determine whether a foreign donation was permissible or not?

Louise Edwards: At the moment we see that they need to improve their processes quite significantly in that area, because they are not collecting enough information to make those determinations.

Q67 **Chair:** Your view is if they are not collecting people's addresses and



HOUSE OF COMMONS

proper information about whether the bank account is linked to the address, they cannot know whether that is a permissible donation or not? They cannot know whether that is a British-registered voter living abroad, or whether it is just someone abroad?

Louise Edwards: It is a huge risk, yes. That is why the first recommendation we made is that they need to go back and look at the payments they have received over or under £500, and they need to satisfy themselves that they are sure those amounts of money are permissible, and if they are not, they need to forfeit those amounts of money.

Q68 **Chair:** When they have said that they have a very large number of people making small donations, those could be people making large donations in lots of small forms, and that could be a lot of foreign money mixed in with other money as well, but there is no real way of telling where all this money has come from?

Louise Edwards: They could be or they could not be; the party needs to go back and work that out.

Q69 **Chair:** It sounds like, from what you have said, in terms of the money they have received from online donations, you cannot be satisfied how much of that is permissible and how much of that is impermissible.

Louise Edwards: Again, it is for the party to satisfy itself of that and we will be watching them do that work. I do not want to give the impression that we are saying there is something wrong with every amount of money that this political party has raised, because we are not in a position to say that. What we are saying is that there is a very clear risk, it is a high risk, the party needs to look backwards and work out what has happened in the past, and it also needs to look forwards and improve its systems so that it has proper procedures in place. If it does both those things then we think that high risk we see at the moment will be significantly mitigated.

Q70 **Chair:** Just before bringing in other members of the Committee, you said there is a high risk here and there is a lot they need to do. The risk, as you have laid it out, would be that using technology like PayPal—and there are other products as well—the money can be quickly wired in from anywhere in the world and that money can add up very quickly to quite large amounts of donations. From what you are saying, it sounds like there is no system in place at the Brexit Party to identify where money is coming from.

Bob Posner: Just to build on what Louise has said, the onus is on political parties not to take money as donations unless they are satisfied they are permissible monies within the rules of the UK; basically, from someone on a UK electoral register or a UK company trading in this country. There is a 30-day period in the legislation after a party receives the money to do those checks.



HOUSE OF COMMONS

If a party cannot satisfy itself it either has to, within the 30-day period, return the money, or if it finds itself after the 30-day period with the money, and if that money appears impermissible and should not be accepted, or there is any doubt about that, then, as Louise alludes to, in fact the party should forfeit it back to us and it goes to the Treasury. That is the procedure in legislation that protects from money going into the system that should not be there. This is audit work that we have required the party to do at the moment, looking backwards. We are watching that, and that needs to be done, and done properly.

Q71 **Chair:** You clearly have doubts about whether these donations have been permissible, because from what you have said, and what Louise Edwards has said, you do not believe they have kept records to be able to know for certain whether the donations are permissible or not.

Bob Posner: Absolutely. We are sufficiently concerned to say they need to do this work.

Q72 **Chair:** If it is a requirement on them to make sure they are only receiving money that is permissible, what you are saying is they are not collecting the information they would need to know whether this money is permissible or not.

Bob Posner: That is what they need to sort. That is absolutely right.

Q73 **Ian C. Lucas:** You mentioned forfeiting the money just now. What is the sanction if the political party does not comply with the necessary rules as far as you are concerned?

Bob Posner: The key sanction is an equivalent sum; that money that has been received that is impermissible has to be forfeited. That in itself is a sanction on a party because they may well have spent that money but they have to find the equivalent sum and that is forfeited. That is one sanction that applies.

That either happens because the party recognises it and voluntarily forfeits the money back, or if that is not the case, it has to be done through the court process and court order. That is how that works. Whether there are other offences committed would depend on whether anything deliberate has happened, basically.

Q74 **Ian C. Lucas:** My difficulty with that response is we have had the election already and you are not satisfied that payments made to the Brexit Party before the European election were in compliance with the law. What is the sanction if unlawful payments were made? Does it affect the validity of the election?

Bob Posner: It is important to say that although we have raised questions, high risk and high doubt at this stage, it could yet prove to be the case that they are fine. We must not prejudge that. They have work to do. However, if indeed the rules have been broken, for breaches of what we term the political finance rules for political parties there are no



HOUSE OF COMMONS

additional sanctions that relate to the elections themselves. That is in contrast to the more core electoral administration rules about the running of elections themselves.

In a parliamentary constituency, if the rules are broken the courts have powers to set aside elections in certain circumstances. That does not apply in relation to breaches of the political finance rules. The sanctions are forfeiture or potentially, if there are other offences, there are fines that we can impose. If there are matters of potentially criminal breach, that is where the police would get involved.

Q75 Ian C. Lucas: The position is that, even though payments may have been unlawfully made, that will not affect the validity of the outcome of the election for which those payments were made?

Bob Posner: Not in law; that is correct.

Chair: A number of members of the Committee wish to come in on this subject, not surprisingly. Jo Stevens is first.

Q76 Jo Stevens: Thank you, Chair. Going back to something you both said earlier about the audit that you are doing, who at the Brexit Party is ultimately responsible for the compliance in relation to financial donations?

Bob Posner: That is the registered treasurer of the party.

Q77 Jo Stevens: Who is that?

Bob Posner: Is that Mr Tice? No, I am not sure.

Louise Edwards: No, I think it is Mr Basey.

Bob Posner: Mr Basey.

Louise Edwards: I would have to check.

Q78 Jo Stevens: Okay. Who is leading the audit to try to match up these donations to satisfy you that they are permissible at the Brexit Party?

Louise Edwards: I do not know who, on an operational level, is leading it. However, Mr Basey is the one who is ultimately responsible for compliance.

Q79 Jo Stevens: Okay. At what point do you decide whether you will or you will not undertake a formal investigation?

Louise Edwards: We have made arrangements to talk again to the party once they have had a chance to properly look at the recommendations that we have made, and we are setting a date in a few weeks' time for us to go back and do that. That will be our first chance to see how the party is responding, to see what they are planning on doing about various recommendations, and to see what they have identified themselves when they have gone through their procedures.



HOUSE OF COMMONS

Whether we get to the point of needing to trigger a formal investigation will be based on the evidence that we see at any given point in time. We are an evidence-based regulator and an evidence-based enforcer. We will keep under review the evidence of what is happening, and whether or not we go to a formal investigation will be triggered by that evidence, not by any other particular timescale.

Q80 Jo Stevens: You would not necessarily have to wait until the end of that audit process in order to trigger a formal investigation?

Louise Edwards: It is always on the evidence. If the evidence meets the threshold, that is when we look.

Q81 Jo Stevens: We have talked about the system that should be in place where you are able to match addresses to bank accounts and that sort of thing. Can you tell us a bit about what systems the Brexit Party did have in place, from what you saw? Do they have any systems in place?

Louise Edwards: My understanding is yes, otherwise our recommendations I think would be a little bit fuller. I was not part of the team that went in to look at them. What the team that we sent in went in to look for was areas of risk, because that is what we were there to deal with. We were not there to say, "That is an example of good practice". There may well be examples of good practice, but we were there to say, "There is a risk". Our findings are all focused around the risk areas rather than going through and saying what they have done well.

Q82 Jo Stevens: Mr Posner, my colleague Ian Lucas asked questions about forfeiture of impermissible donations, and you mentioned that the sanction ultimately is court proceedings to recover the monies. Has that ever had to happen in the past?

Bob Posner: Yes, it has had to happen. There are more instances of parties recognising themselves, working with us, that they have taken some money they should not have, doing the right thing and voluntarily submitting it. There are also occasions where matters have gone to court.

Q83 Jo Stevens: You also said that breaches of political finance rules do not result in election results being overturned and rerun. Do you think that they should?

Bob Posner: That is a matter for you politicians in Parliament. It is an interesting anomaly, though. There is a clear difference. One would need to take the view that fraud and corrupt, illegal practices can be such that a court can say that an election is null and void and needs to be rerun. We have seen that sometimes in parliamentary constituencies over the years, occasionally—not very often, just occasionally. The question is for the political finance rules, which were written in the late 1990s—much more recent than the traditional electoral administration of 150 years. What is the right level of sanction when those rules are broken? That is a policy question for Parliament.



Q84 Jo Stevens: Sure. I have a lot of constituents say to me that they find it astonishing that, for example, in the referendum in 2016 there were clear breaches of electoral law that took place and yet the result still stands, and then you look at examples where parliamentary constituency elections have had to be rerun because of what would appear to be much more minor breaches. Do you think that this is something that the Government should be looking to update electoral law on?

Bob Posner: We have made a number of recommendations that could be framed within the current system. We have a toolbox of investigation powers, and those are good powers, but there are limitations on those.

One of the limitations is our ability to get information quickly from third parties, if you like. That could be social media platforms, it could be other organisations, and so forth. We have said it would be sensible to have, like other regulators in other fields have, the ability for us to get all that information more quickly, and we would need additional power to do that, additional investigative powers. That seems to be a sensible thing to do that would help everyone.

The other thing we have said is what one wants is suitable deterrents. We do not want to end up imposing large fines, because in a sense that means something has gone wrong and one is imposing something after the event. It is much better if one has suitable deterrents to deter people from breaking the political finance rules.

As things stand, as I am sure you know, we have a maximum fine of £20,000 per offence. When one compares that to other regulatory fields, the Information Commission and so forth, that is very low. Truly, that is not going to be a deterrent to someone who recklessly, negligently, or deliberately goes around breaking the political finance rules. One can do things in the current system to hopefully make it better for everyone, not looking to ever have to impose those big fines, hopefully, but as a deterrent.

Q85 Jo Stevens: If somebody, for example, donates £6 million, £7 million or £8 million to a political party and knows that if that is outside of the rules there is a maximum of a £20,000 fine to that party, that is not much of a deterrent, is it?

Bob Posner: We do not think so.

Q86 Julian Knight: What was it that prompted you to engage with or investigate the Brexit Party? What were the signals that made you go and send your team in?

Bob Posner: This was a new party, clearly a new party of significance, that was very quickly clear, and from the beginning we were in contact with them. Political parties have to apply to us to set up a party, so we were in contact from the very beginning with them. Certainly, they worked well with us at the beginning in enabling themselves to be set up.



Q87 **Julian Knight:** You said, "At the beginning".

Bob Posner: I did not mean that in the sense of not now; "From the beginning" would be a better phrase. In that sense we were very aware of what they were doing. For us it is very normal to keep a close eye, particularly on a party that is going to be potentially quite significant, on how they are setting themselves up. We gather our own intelligence. We were on a course of action where we already had concern, and that lead to us taking the action. For us, we think it is important not to delay if we do have concerns. We do not delay with any party; we sort out the party as quickly as possible.

Q88 **Julian Knight:** They are a new kid on the block and you wanted to check them out, basically?

Bob Posner: Yes.

Q89 **Julian Knight:** What about Change UK then? You say in your FOI, "As regulator, we talk regularly with parties and campaigners, but we have not made any 'findings' —" in the same way you have with the Brexit Party — or recommendations about funding in relation to Change UK, People's Vote or Our Future Our Choice."

In relation to Change UK, many of the things that you have said about what prompted you to look at the Brexit Party—it almost seems incredible now to think that you could apply them to Change UK, but there was a short period when you could think that they were a significant party and a significant movement. I am just wondering whether or not you think that you applied the same parameters as vigorously to Change UK as you did to the Brexit Party?

Bob Posner: Absolutely. People are understandably concerned about whether the Commission is impartial. We might be regulating against one political party or viewpoint, and they might say, "Why are you not regulating against the other lot", I suppose.

Q90 **Chair:** I will just interrupt for a moment, if possible, to say that Arron Banks has threatened to sue me, he has threatened to sue the Electoral Commission, he has threatened to sue *The Guardian*, and he has threatened to sue Channel 4. The great thing about the way this Parliament works is that people can speak freely without fear, or favour, or intimidation from wealthy businesspeople who like to throw their chequebook around. We are grateful for your evidence, and hopefully you can answer our questions fully.

Bob Posner: Okay. Good. That is helpful. We are vigilant—and why would we not be—and impartial in all we do. We worked with Change UK very closely at the beginning when they applied and, indeed, we will be going back and checking their systems as well.

However, there is no indication that we should have gone into their premises before the election. There was no reason to do that, so we did not do it. We act on the evidence, as Louise was saying earlier. I am



HOUSE OF COMMONS

confident of that. Where there have been allegations of impartiality about the Electoral Commission, they have never proved to have any basis, I have to say, and long may that last.

Q91 **Julian Knight:** When you say “indication” and then you apply that to Change UK and not to the Brexit Party, what is the indication that was lacking with Change UK that was present with the Brexit Party?

Bob Posner: All regulators in all fields obviously keep an eye on the wider picture of what is going on among those they regulate, and all regulators gather their own intelligence and their own information. We are no different. It is not something one openly publicises or speaks about but it is what we do, it is what you would expect any regulator to do; we come to our own views. Often that is informed if, indeed, there is stuff in the public domain, but equally we do our own work.

Q92 **Julian Knight:** That sounds all fine about intelligence, but it does sound to me as if you are skirting around the issue just slightly. I need to get to the heart of this, basically. When it comes to Change UK there are many grounds that were very similar to the Brexit Party.

Why is it that you felt compelled to put a team into the Brexit Party but not into Change UK? What is it they were doing differently, or better, or that you were assured about? Was it to do with what had happened potentially in the past and some of the investigations that you have undertaken over the last couple of years in terms of money and trail of money? I am still not certain why your investigation, or your examination, has been more forthright in their instance than it is with Change UK.

Bob Posner: We are evidence led. Louise might want to add to this; I can see she does. We do not just investigate on a whim. We investigate for a reason. I should not use the word “investigation”, because the Brexit Party are not under investigation. I made that clear earlier. But we do not look into matters. We are always looking to assist parties to comply.

We had reason to go into the Brexit Party; we went in. That was proved right. You can see from what we published there are very serious concerns and we hope to work with them to put them in the right position. That is our intent with any political party. We do not have an evidence basis or any reason to think at this stage there is something wrong or any reason we should have gone into Change UK. We constantly look at matters. We constantly keep matters under review. Do you want to add to that?

Louise Edwards: Yes. I want to make clear it is not a compare and contrast game. We do not take two political parties and then compare and contrast how they are working. What we do is look at each one individually to try to take a decision on the evidence as to whether there is a matter we need to look at.



HOUSE OF COMMONS

As Bob says, we are not formally investigating the Brexit Party. This is part of our oversight work, which is a much broader area of work than the narrow investigatory work that we do when it is needed. One of the reasons why we decided that we would take the action we did with the Brexit Party was that we could see there was a party there that had openly acknowledged a fundraising structure that was focused around small amounts of money. That is fine. That is perfectly legitimate.

Q93 Julian Knight: That was different to Change UK?

Louise Edwards: That is different. It had a leader who had talked about the amount of money they had gained in that way. Again, that is fine. It is good that people are participating and giving money to parties. If you allow small amounts of money to be given that may well encourage more people to participate in politics. However, what you have is a layering effect with a newly registered party that has a lot of money coming in through a fundraising structure that does have risks attached to it. Then there is some analysis done by people in the media and elsewhere who have tried to use the PayPal system and point out things like, "I did not have to put an address in" or, "I did not have to match it up with my bank account details".

Then you have a party that is currently spending money in a national campaign. There is a very live and current issue there. It is raising money at that point, it is spending money at that point. These are all factors that layer together and make us think, "Hang on a minute, we need to take a different look at this. We need to go in and we need to talk to the party". That is what prompted us then to speak to the party and say we were going to conduct this review, which the party agreed with and allowed us to come in and do this work.

Q94 Julian Knight: It was a combination of the fact that there were lots of small donations and the PayPal system. Is the PayPal system active with other political parties?

Louise Edwards: Yes, a number of parties use PayPal. We have not looked at all 400 parties on the register, but we have done some work looking at some of the major parties, including those represented on this Committee, and pretty much all of them do use PayPal. It comes back to what I was saying before. PayPal is a tool. It is a tool that is set up and configured by the parties. The people responsible for making sure they are complying with the rules are the parties. It is how they configure these systems that is important for us, to help them meet their legal obligations.

Q95 Julian Knight: You are happy with how the main political parties deal with PayPal? Is there anything different between how the Brexit Party deals with PayPal and other political parties deal with PayPal?

Louise Edwards: Yes, there is quite a lot of difference, hence the recommendations we had to make to the Brexit Party.



HOUSE OF COMMONS

Q96 **Julian Knight:** It is to do with the addresses, the names, and the non-disclosure, whereas with other political parties it is disclosed?

Louise Edwards: It is all those sorts of elements, yes.

Q97 **Julian Knight:** Thank you. More generally, just to change tack slightly, are you aware of any trends towards political parties accepting crypto currencies?

Bob Posner: To our knowledge, only what we know, that is not in major use by political parties in the UK. There are some interesting instances overseas in some countries. Use of crypto currencies does happen. We issue some guidance on that. We have assisted political parties on how to use it. It is another means of collecting money. Louise, do you want to come in on that?

Louise Edwards: Yes. I think you really hit the nail on the head at the end there; it is another way of collecting money. It is a way that the current legal framework applies to as it would to any amount of money. It is something that can be valued at a given point in time, checked for permissibility, it can be accepted, and it can be reported. It is just another way of doing it. We do not see it a lot. There were a few isolated examples from 2015. I suspect one of the reasons we do not see it a lot is because there are not many places you can spend crypto currencies. That might be a factor that changes over time.

Again, it is a tool. It can be used in a way that is very transparent; indeed, some of the online ledgers for crypto currency can give real-time transparency. Alternatively, it can be set up in a way that is not terribly transparent, with closed ledgers. Again, it depends on how it is set up and how it is used. We do have guidance on it, but so far it has not come to our attention as a significant trend in the UK.

Q98 **Julian Knight:** Okay. You mentioned international comparisons. Do you believe there are risks associated with this type of donation that are specific to this type of donation?

Bob Posner: It is certainly a means of funding political parties that can be used in a way that is perfectly proper and that would work within the UK rules and laws. The risk is that it is used in a way that is not consistent with that. Louise referred to closed groups and so forth, and maybe encryption systems like that that make it difficult. This goes back to, in any jurisdiction, what power and reach one gives to regulators to investigate and obtain information quickly from organisations and to act on it.

Q99 **Clive Efford:** I will follow up on one or two things. Do political parties co-operate fully with you? Are some better than others?

Bob Posner: I would definitely say that in the UK we have a culture of compliance. Basically, most parties want to comply—it is about complying with the rules, and why would they not? Their reputation is at stake, and



HOUSE OF COMMONS

that is a good thing, and that is how things are in the UK. We do not want to give any impression that political parties are setting out to break rules in any way at all. Equally, there are times when political parties work close with us to make sure they do comply with the rules—generally that is a good experience—and there are other times where we have to use enforcement powers and it is more about us being rigorous about enforcement.

Q100 Clive Efford: When you first raised your concerns about the Brexit Party they were fully co-operative with you, were they? They did not ignore anything you said? They were responding to every request you made?

Louise Edwards: Yes. Our first approach to them on this particular decision to go into the review was to explain that that is what we were going to do. The party were receptive to that. We agreed a time and venue to come in.

Q101 Clive Efford: How early from when they were set up did you become concerned about their donations?

Louise Edwards: “Set up” is a difficult one, because I am not entirely sure when the party set up. I know when it was registered, but it could have been set up before that. We first had a regulatory interest in this when they applied to register as a political party. Very early in their registration we asked them to come in and see us so that we could talk to them about the obligations that were on them about their compliance processes, opened up that dialogue really right from the start when they were registered, and then we have had ongoing discussions with them since then.

Q102 Clive Efford: Do you think that you need any sorts of powers to place requirements on parties much earlier, given the exchanges you have had about the election is over and now we are trying to pick up the pieces? Should you be able to intervene earlier and require parties to take certain actions?

Bob Posner: It is certainly our aspiration, and I think everyone’s aspiration, that the sooner one can address problems the better for everyone, and that could just be helping the party to comply and get things right. If that can be done before an election is held, of course that is better. In some fields of regulation—I refer to other fields of regulation—the health regulation is a good example: the way the health regulators work is that they act immediately. They go into premises unannounced if something needs to be done. Of course, those are life-and-death decisions; one understands that. It is interesting to think about in the political field.

You would clearly want elections to run without the regulator interfering. Political parties have to do their job. That is what campaigning is about, and so forth, but equally one wants a regulator that could be suitably active and could take action as necessary. I think when one looks at our ability to do that, we have made some recommendations for some more



powers, which I have referred to and which I think are proportionate, but also I think there is probably something about a change in culture, which is whether it is the political will, whether it is Parliament's will, that we do more of this work.

If that becomes more accepted, then clearly it is easier to do. The contrast is that one has to do it on the back of court orders and warrants, and that is not best. It is best if one has a co-operative compliance approach to things.

Q103 Clive Efford: Okay. Can you share with us your reflections on the lead-up to the recent European elections? Have you, for instance, observed any particular trends on social media?

Bob Posner: I will start at the broadest level on the European elections and I will come to digital. Clearly, these were elections a lot of people said would not happen. For us as an organisation these remained scheduled elections and it was our job to plan for them to happen in case anyway. We took a lot of criticism for that, for preparing in case they happened, but we did what we could in advance.

There is no doubt that it was very, very late in the day that it was acknowledged by Government that these elections would happen, and that funding was forthcoming for returning officers and electoral registration officers. It was very late in the day that political parties acknowledged, in a sense, they were going to happen and got themselves up and running on campaigning and so forth.

All that had an impact, including on social media campaigning, and not a positive impact. We will be reporting on these elections. It is part of our statutory job to report on all elections. We will be reporting on that in due course. There were issues. Broadly, I think, returning officers across the country did very well to run the elections well, but there were issues. We all know the issues about non-UK-based EU citizens. It is hugely unacceptable that people who wanted to vote could not vote. I have great concern and empathy for them and so does the Electoral Commission, that is hugely unacceptable. That was entirely avoidable had these elections been prepared for earlier and been recognised they could happen.

We all have concerns about UK citizens overseas who also had difficulty to vote because of the system and getting ballot papers out to them and back. Again, we made a recommendation to have a much more straightforward system that would help that. These were things that were avoidable. We think of voters; I am sure we all do. When people want to vote and they cannot vote, that is extremely disappointing and concerning.

On these European elections, to come back to your social media point, one of the other things that happened was in the normal course of events, a long time before these elections, probably a good year in the



HOUSE OF COMMONS

lead-up, like the rest of Europe we would have been preparing for these elections, and there was a lot of co-operation across nations with social media in mind among the other states of Europe in the EU, co-ordinated by the EU Commission to help do that.

There was a voluntary code of practice the EU put in place for social-media companies, and there was a lot of interaction. In the event, because the UK was so late to come to the table, the UK did not participate in any of that preparatory work. That is not helpful, it has to be said, and that has an adverse effect. The Commission is working very closely on that now. We have met with the Commissioner concerned last week, so we will tap into all that work about lessons that can be learned. What we have to do, because there has been little work in the UK on what happened on social media on the European election because we were not part of the network across Europe, is to watch very carefully what the conclusions are of other countries in the EU and learn from that.

Clive Efford: Okay. Facebook, Google and Twitter started to give advert reports. Do you have any idea how that worked, whether that was a success, and how the public reacted to it?

Chair: Sorry to interrupt you, Clive. This is a very important line of questioning. There are a lot of people who want to come in on the payment side of it so we will just conclude that first and then I will come straight back to you after that.

Q104 **Brendan O'Hara:** Following on from what Mr Efford was saying, when you met the Brexit Party initially did you get the impression that they were naïve or unaware of the legislation?

Bob Posner: I am just going to say simply, no, I did not have that impression, we do not have that impression. I did not meet them personally, but we do not as an organisation have that impression.

Q105 **Brendan O'Hara:** You did not get the impression that they were unaware of their responsibilities?

Bob Posner: No. Part of our registration process for any political party is to make sure that they are aware of their responsibilities. We do not register political parties without being very clear to them that there are rules to follow, they have to have a constitution and a financial scheme. That is part of the process. Sometimes a political party involves people who are new to the scene, in a small party set up with people who have never experienced the political arena. I do not think it would be right of me to say that is the case with the Brexit Party.

Q106 **Brendan O'Hara:** Okay. As far as you are concerned they were aware of their responsibilities when you met them?

Bob Posner: I would have thought that was right. I would have thought they would agree with that.

Q107 **Brendan O'Hara:** How surprised were you when you realised there were



HOUSE OF COMMONS

gaping holes in the procedures, given the fact that, while they may be a new party, they are not a new set of politicians? How surprised were you there were gaping holes that existed in their procedures?

Bob Posner: We do not make a value judgment about surprise. We are a regulator, we just get on with the job, quite honestly, and we do not judge people in that way. What I would say, and it goes to your earlier question, we went into their premises, and for me as chief executive in the week leading to that it became pretty apparent that we had concerns, we needed to do something and we were on that route.

Q108 **Brendan O'Hara:** Would it be safe for me to assume, without putting words in your mouth, that you would have expected a far more robust procedure to be in place by a political party basically made up of experienced politicians?

Bob Posner: Absolutely. We are on record, it was published, that we have dissatisfaction with how the arrangements were put in place. It is important, I stress again, there are no current findings they have breached the law at all. We have expressed very clearly that high risk. The next stage is to establish whether something went wrong or not.

Q109 **Brendan O'Hara:** Okay. But they are not naïve? Okay. In terms of the audit, how many people from your organisation are working on that audit?

Louise Edwards: The team that went in comprised of three people but they are supported back in the office by a senior management team or by professional lawyers, or whoever it is. I am not sure I can give you an actual number; it is more just the number of people who need to input into it.

Q110 **Brendan O'Hara:** Are they working from your office or are they embedded with the Brexit Party's HQ? Where are they working from?

Louise Edwards: They are working in our office, yes.

Q111 **Brendan O'Hara:** Working in your office. Are you satisfied that working from your office they have access to all of the information that they need?

Louise Edwards: When we went in and did the visit that we did in May and then brought information back to the office, we were happy that we had enough information to make the recommendations that we did. Now what we have done is put them back to the party, and the party needs to reflect and make changes.

As I mentioned earlier, we have another discussion in train with them in a few weeks' time to see where they are at. That will be the point where the team will say, "Right, what do we need to see now? Do we need to see the new procedures? Do we need to go back? Do we need to call them into our office?" It is at that point when we will decide what the next appropriate step is.



Q112 **Brendan O'Hara:** Is there anyone from the Brexit Party who is dedicated to working alongside your team?

Louise Edwards: We have been dealing with the treasurer. He is the one who is responsible for these matters. What decisions he takes about how operationally within his party he wants to take them forward is a matter for him. At the moment, it is the treasurer that we are talking to.

Q113 **Brendan O'Hara:** When would you expect, roughly, your team to be able to report? Are they doing a report on this?

Louise Edwards: We are expecting to talk to the party again in a few weeks' time. Some of the recommendations that we have made are more urgent than others. We have made that clear. Some are high risk, we expect things to be done pretty quickly. Some may take the party a time to reflect on and to work out what it wants to do next. We will have to keep talking to the party about that, keep talking to them about how long it will be before they think that they have addressed all of the risks.

Q114 **Brendan O'Hara:** At the end of it, do you think that we will get to a situation where you will be able to find out exactly how much money the Brexit Party received while, in your own words, at risk of non-compliance? Will a figure ever emerge of exactly how much went into the Brexit Party while they were in that state of non-compliance?

Bob Posner: What will emerge, it is our job, is an absolute position from the regulator. Sometimes that can be precise on figures, sometimes that is framed in a way to say that one cannot be satisfied that sums of money were permissible, there is not the evidence to show it was permissible, and under the legislation, therefore, it should not be accepted. We will be as precise as we can be but sometimes there just is not the information to get to every bottom figure.

Q115 **Brendan O'Hara:** We have a situation of a single-issue organisation emerging for a single campaign, into which money floods, both permissible and impermissible, and which there is no way of telling which is which, they then spend both the clean and the dirty money on a successful campaign, and then you guys go in and you say, "You had better clean up your act", and they say, "Okay, we will clean up our act", but by that time the damage has been done and all you can do is then issue a relatively small fine. As legislators, how would you advise us to avoid that situation happening again?

Bob Posner: You are right to identify those risks, and those are risks in our system. What I would say as the regulator is what you want to do is empower the regulator with the right powers, the right reach, to act and to act swiftly. That is about scope to get information quickly from anyone who potentially should be providing information to the regulator and real deterrents that can be imposed quickly with fines and sanctions that do hurt appropriately to deter breaches of the rules.

Q116 **Brendan O'Hara:** Do you accept that the legislation as it is currently



framed is absolutely no deterrent to this kind of behaviour?

Bob Posner: If you are referring to where laws are broken and our ability to do something about that, we do investigate, we reach findings, we have done that, we have imposed maximum fines, and those maximum fines are very low at £20,000 per offence.

There is, of course, also a range of criminal offences where people have been potentially criminally culpable. Those matters currently get referred to the police for them to investigate. There is always another debate, which is: how far does one enable a regulator to take forward criminal matters as opposed to asking the police to take it? Either option is good; the police can take it or the regulator can take it—it really comes back to where everyone is, whatever culture, or nation, or jurisdiction one is in, what is the best in that sort of context.

Q117 **Ian C. Lucas:** Do you think it would be sensible for you to have the power to issue a certificate of compliance to a political party before they were permitted to participate in an election, so that we could check that the compliance is satisfactory before a national party participates in an election?

Bob Posner: I think it is an interesting idea. It is not one I have come across or that we have a position on, I have to say. My initial comment would be that if that was a good thing it would be a certificate of compliance at a point in time. What it does not do is answer the fact of what happens after that point in time. It still might be a reassurance that at that point in time the parties reached a particular standard but it would not deal with what happens after that. The sanctions would.

Q118 **Ian C. Lucas:** Indeed, I accept that. It would mean that before a political party took part in a national or international election there would be, at the point of time before they participated, a statement from the Electoral Commission, for example, that they were complying with a satisfactory level of financial arrangements before they could participate in the election.

Bob Posner: This goes back to the principle of how much regulatory oversight feels appropriate in the UK in the context of our politics. Are we at a stage or time where we would want the regulator to do that—I do not have a view on that—or is that a step too far? Politics happens and it is important new political parties should be formed and there should be participation. This is a judgment whether we want that extra layer of protection. That is for Parliament.

Q119 **Ian C. Lucas:** I want more protection than we have at the moment when someone who makes unlawful payments is permitted to benefit from those unlawful payments by winning an election. I find that an extraordinary state of affairs. Don't you?

Bob Posner: It is certainly our job, our desire and our effort that people should comply with the rules.



HOUSE OF COMMONS

Q120 **Chair:** A couple of final questions from me on this. In the document we published today, in the notes you have on the PayPal system, one of the high-risk areas identified where you have recommended implementation as soon as possible was the requirement that the Brexit Party should use security-prompt systems when receiving payments, like Captcha, which helps identify whether the person making the transaction is a real person versus being a bot. Given that is one of your high-risk recommendations, are we to assume that the Brexit Party does not have a system in place to determine whether a transaction has been processed by a bot as opposed to by a human?

Bob Posner: I think that assumption is right, Louise?

Louise Edwards: Broadly speaking, yes. PayPal may have various procedures that could be activated by the party if it wanted to, but that was not one of the ones it was using.

Q121 **Chair:** No. The exact words on the note are, "We also recommend that the Party uses a system that requests all donors to complete a 'Captcha' or security prompt", so not just Captcha. It was suggested that there is not a requirement that they complete a security prompt before the payment was processed.

Louise Edwards: Yes, that is right.

Q122 **Chair:** In the same way that you have raised concerns that it is possible there could have been impermissible foreign donations, or donations over the £500 limit because proper records were not being kept, it is also possible that they could have been receiving payments from bots as well?

Louise Edwards: It is possible. I just want to echo some of the points that Bob has made, that it is also possible that has not happened. This is why it is really important that the party goes back and does the audit that we have asked it to, and reports to us on that, and tells us what it has found.

I do not want to make suppositions either way. What we have identified are risks, and risks that need to be addressed quickly, but we have not conducted a formal investigation and made any findings that the rules have been broken at this point.

Q123 **Chair:** What we can say is that, from the Electoral Commission's assessment, the Brexit Party had not put systems in place to make sure this could not happen. The question is really whether it happened and to what extent.

Louise Edwards: Whether or not it has happened and, if so, to what extent is what that audit is going to have to look for.

Q124 **Chair:** Yes. If someone had wanted to create a bot network to donate money to the Brexit Party, the Brexit Party systems would have allowed that?



HOUSE OF COMMONS

Louise Edwards: I do not know. That will depend on the facts of that particular area.

Q125 **Chair:** You are saying it has not been audited so we do not know if it happened. I am saying, if someone had that intent to use a bot network to donate money to the Brexit Party, there is nothing in the systems the Brexit Party put in place that would have necessarily identified that and stopped it happening?

Bob Posner: To our knowledge, that seems a possibility.

Q126 **Chair:** That is a possibility?

Bob Posner: Yes.

Q127 **Chair:** Yes. You mentioned earlier, Louise Edwards, that you thought the money laundering regulations should apply to political parties. I wonder if you could say a little bit more as to why you think they should?

Louise Edwards: Sure. The money laundering regulations themselves are focused on financial and other institutions. It is something that needs consideration into how it might work; I am not suggesting that you can simply expand it. It might need some thought, but the anti-money laundering regulations require things like written assessments of money laundering risks and training to be given to staff who handle money about the possibility of money laundering. It requires additional checks over and above simple permissibility, what is known as know-your-customer checks.

These are all very sensible, very straightforward procedures that we think could be put in place with most political parties to take that further step. At the moment, they are not a requirement on political parties. It seems to us that that is a very straightforward area that could be considered.

Q128 **Chair:** If they did apply to political parties, do you think the Brexit Party would constitute a money laundering risk as it currently stands?

Louise Edwards: That is a hypothetical. I am sorry, but I cannot answer that.

Q129 **Chair:** If that is based on the fact there are not proper procedures to identify where money is coming from, how much money is being donated and whether it is being processed by real people or bots, all of those things would be considered to be a money laundering risk, would they not?

Louise Edwards: The challenge I have is by saying "risk" you could be talking about a low risk, a high risk, a medium risk, whatever it is. Any organisation might be at risk. Even an organisation that has the best compliance with anti-money laundering regulations in the world could still be at risk. It is really difficult for me to answer that because the money laundering regulations are not in force, so it is not an area that we looked at in relation to this party.



HOUSE OF COMMONS

Q130 **Chair:** You have listed things you think are high risk about their systems, and all the things you have been talking about are areas where you believe the parties are high risk. I just wonder, given you have made this recommendation, which the Committee may wish to even take forward and put to the Government that the money laundering regulations would comply, the logical deduction from that would be that you believe, looking at parties like the Brexit Party, that there is a vulnerability, there is a risk of money laundering, if they do not have proper systems in place.

Louise Edwards: For any party that does not have systems in place, yes.

Bob Posner: Yes.

Q131 **Chair:** Yes. We are talking about a party that does not, so we would have to assume in that case you believe the risk applies there too. Is that the case?

Bob Posner: Yes.

Chair: Yes. Thank you. That covers the questions on that particular topic on micropayments. Let us go back to Clive Efford now. Sorry to interrupt you.

Q132 **Clive Efford:** I will make just one last comment if I can, Chair, which is: as someone who fights elections, and has done all his adult life, I hope that when I am fighting an election the other guy, or the other person, is fighting on the same rules as me.

What I find about that question and answer session just now is that the reaction is all too slow. The election is done, and we are still trying to pick up the pieces. You do not have to comment on that, but it is astonishing, really, to sit here and listen to you raising those concerns that you have no powers whatever of enforcement to make sure somebody was compliant. That is something the Government and Parliament need to go away and have a serious look at.

Anyhow, let us go back to digital campaigning. Facebook, Google and Twitter put the advert reports in place. Do you have any feedback on how that may have affected the election or how the public reacted to that?

Bob Posner: Yes. I should have said earlier in my general answer to your question that we have been in close contact with the major social media platforms for quite some time, working with them, and encouraging them to put up the advert platforms and so forth. Certainly in the lead-up to these elections in May, the European and local and so forth, we have been looking very closely at what they had provided, how all that works and what parts of what they are doing has not worked that well. I know Louise has some thoughts on that. Do you want to add to that?



HOUSE OF COMMONS

Louise Edwards: Sure. We are still evaluating, and part of that is because for us the election is not over yet. We have the returns of spending to come in. The first deadline is in August, the second deadline is in November. That is when all political parties should have reported their spending to us. One of the things we want to do is crosscheck that against the ad library. Our full evaluation of how well they have worked we cannot complete yet.

We do have some emerging views now. One of the areas we have been looking at is about the public, the voters and how they have worked for them. Some of the thoughts we have there is: undoubtedly it is the case that there is more transparency in this election about spending on social media platforms than there has been in the past. I do not want to take away from that. That is a very good thing. Could there be more transparency? Probably.

The first words I want to say are “in print”, because while the ad libraries exist, they are not linked to user’s newsfeeds. What would be much more valuable when you are looking at an ad is to see on the face of the ad who has paid for it, rather than needing to go and look at an ad library. One of the other areas we are looking at is it is not always immediately apparent from the person whose name is on the ad whether or not they are affiliated with a particular political party. You could have somebody who pays for an ad in their own name, for example, but actually is affiliated with a political party, and there is no requirement to declare that.

The other thing that we are looking at from the perspective of the voter is a lot of these organisations have something that says, “Why am I seeing this ad?” You do not get terribly detailed information. You get some information, that is good, but you might get information that says, “I am seeing this ad because this person wants to target England”. That is something but it is not telling me an awful lot as the person who is seeing it.

We are looking at it from the voter’s point of view. From our point of view, we think that the information around targeting again is not sufficiently granular. It is more helpful than not to know this ad was targeted at England but when you are talking about a regional or constituency structure there is probably a level of granularity that would be more helpful than just a very, very high level one.

One of the other areas that we are talking to companies about at the moment is how they define political advertising. They have quite a broad definition. It definitely catches things that are not controlled election spending but it also does not capture everything that is controlled election spending, particularly around single-issue campaigns that non-party campaigners may be running.

We want to look at what the impact is of that particularly and we will be able to see that when we start to look at spending returns as well. Are



HOUSE OF COMMONS

these ad libraries actually showing everything that we would consider to be controlled political advertising or not? There is more work to do. Those are just some of our emerging conclusions at the moment. We will have to wait until we can get to the bottom of some of those issues.

Q133 Clive Efford: Will the Government's imprint rules address any of the issues you just outlined?

Louise Edwards: The proposal to bring in the imprint on electronic material?

Clive Efford: Yes. The announcement on 5 May.

Louise Edwards: Yes, is the short answer. Yes.

Bob Posner: We welcome that, of course. What none of us has seen yet is the detail of how they are going to do that but we welcome the intent to do it. We look forward to working with Government to get that right.

Q134 Clive Efford: Just so I am clear: you have outlined quite a number of issues there around imprinting and the information that people are given about why they are receiving adverts. You believe that the proposals that the Government announced on 5 May about imprinting and further information address all of those issues? Do you think they need to go further?

Bob Posner: I think it is right to say that none of us have the detail of exactly what they are going to do. The principle is absolutely right and it is good the Government has said that. We will need to wait and see exactly to what extent and how they are going to address it.

Q135 Clive Efford: Just one last question. We have had issues with social media platforms, Facebook and others, about their failure to check up on what is going on on their platforms and taking the money and running for the adverts. Is there more that you feel that they could do?

Bob Posner: We welcome the approach and the direction of travel that social media companies should carry more responsibility and more duties. The Government is proposing an online harms regulator. They have spoken about codes of practice and some duties on social media platforms, for example. In principle, we welcome that. That must be right.

I would say that whether there is an online harms regulator or not and whatever is put in place, what that does not do is answer the sorts of things we have been discussing and many of the things you as a Committee have been saying as recommendations. That is not a replacement or a substitute for that. Many of your recommendations and many of our recommendations still need doing in the context of election law, political finance and election law, and what we would like to see is the two working together well.



HOUSE OF COMMONS

We could see that potentially an online harms regulator could put certain responsibilities on, for example, social media companies, with how that might impact on electoral law in mind, but then we need to do our job on regulating those rules properly. You have made a number of recommendations about that. We have as well. I think there is a parallel set of recommendations that have to be implemented.

Q136 Jo Stevens: We had the referendum in 2016 and all the findings that you had arising out of the co-ordination between the Leave campaigns and unlawful conduct. We have had a general election since then. We have had the problem in the European elections with citizens of EU nations being unable to vote and British citizens overseas not being able to vote. Do you as the Commission do any work with members of the public on how confident they feel about the integrity of our elections and referenda?

Bob Posner: Yes, we do. Thank you for the opportunity to mention that. We do a lot of voter survey work after elections and on an annual basis. I will over-summarise but basically people want there to be an appropriate level of regulation, they want to be sufficiently informed so they can make the right choices about how they vote, but there is a lower satisfaction and confidence about the rules being enforced and there being sufficient rules. The views of this Committee and many politicians' views that more needs to be done are absolutely consistent with the public view, from what we can see from our voter survey work.

Q137 Jo Stevens: Do you think the Government has acted quickly enough? You published your report in June 2018, I think, with recommendations. You also, after the 2014 European elections, made recommendations that were not acted upon, which I think would have negated that risk of EU citizens not being able to vote. I suppose what I am asking is: do you think Government have treated this as an urgent issue or could they have done better?

Bob Posner: We always want Government, whatever Government, to implement our recommendations. We think they are the right recommendations. At least we want them to be debated and responded to and for Parliament to consider them. It is frustrating for us when fresh sets of major elections arise and what we think are important recommendations and changes that could be made have not been made. I do not want to lay it at the door of any particular Government or the current Government because it goes back a number of Governments, quite honestly, where things have not been put in place that could have been put in place.

Jo Stevens: Thank you.

Q138 Chair: Just a final question from me. It has been pointed out that Facebook's own platform policies identifying political advertisers only work if you see the ad as originally posted by the advertiser, and if you share that advert any kind of trace as to who the advertiser is disappears



HOUSE OF COMMONS

from the system. I wondered if this is something you have looked at. Do you believe that this is a glaring error in the system that needs to be corrected?

Bob Posner: That is interesting. I am not sure I have given that aspect direct thought. There is an issue we are very conscious of about traceability and archiving. Adverts appear and then disappear, as it were, which may be part of what you are saying. I am not sure. We are very concerned about that. We are concerned that there should be the record. It is very important that after the event, the people who look into it understand what happened, as well as the before as well. Both are as important, in many ways. Currently, yes, they might be in the advert libraries but then they disappear, for example, because they just take the information away. There is something that is not right currently.

Some of Louise's points about the platforms working differently, where people are targeted they do not have to go to advert libraries because there is something straight there on the thing on which they are targeted. They can see who is influencing them, or there is a direct link and they can go and look at it, as it were. That is a very powerful tool. That in many ways could be a better way to approach things, or part of it, therefore raising people's digital literacy and understanding of things.

Q139 **Chair:** Yes. It shows, to my mind, why we need to change electoral law to set this. Facebook have introduced a platform policy that superficially sounds like it is going to make ads transparent but—as you have identified and the Information Commissioner identified as well—the named person is not necessarily the true source of the funds or the true organisation. Indeed, if someone sees an ad and then shares it, the traceability link even as it stands at the moment disappears. Facebook's current policy is to give a false assurance, in some ways, that transparency is being provided.

Bob Posner: Yes. We want to see more and better. It is good that something has started but there is more to be done. We work very closely with the Information Commissioner.

Can I also just add, slightly tangentially, that when people talk about the reform of electoral law, we do not really support what I would say are ad hoc individual reforms here and there? We think electoral law is so important that when it is reformed it is important to look at an area of electoral law as a whole. Digital could be looked at and so forth.

What we find difficult sometimes is where the system gets tinkered with and a little bit gets changed in a section and so forth, which often has unintended consequences. We do very much support proper reform of electoral law, comprehensive in the sense of areas of electoral law, but not, "Oh, there is a problem. We will just change this subparagraph in this section". That tends not to be a good solution. That tends to go wrong because it is something that is very carefully balanced for a broadly even playing field and for broadly fair rules.



HOUSE OF COMMONS

Our policy stance or our position is that when we make sets of recommendations such as the digital recommendations we made last year—some of your recommendations we also agree with and there was a report by Lord Pickles on a number of electoral fraud matters—we see those as really good packages of recommendations that Government and Parliament can implement, but not to cherry-pick and not take particular things out. We think that is really important.

Q140 **Chair:** Thank you very much. I think that concludes the Committee's questions for the Electoral Commission. Thank you for your evidence this morning.

Bob Posner: Thank you.

Chair: We will now proceed to the second panel.

Examination of Witnesses

Witnesses: Sasha Havlicek, Chloe Colliver, Philip Gradwell and Tom Packalén.

Q141 **Chair:** Good morning, and welcome to the second panel in this evidence session. I wonder if I could start with Sasha Havlicek and Chloe Colliver. Could you please, for the benefit of the record, just introduce the work you have been doing to the Committee and give us a summary of your principal findings relating to the European parliamentary elections this year?

Sasha Havlicek: Thank you so much for having us here. Just a couple of words perhaps on what we have been doing over the past three years. The Institute for Strategic Dialogue has been doing analysis of digital information operations across a range of elections—national elections but also state-level elections, including the Bavarian election. We have most recently done that analysis across the European parliamentary elections. Would it be helpful to say a couple of words about the methodologies we use?

Q142 **Chair:** Indeed.

Sasha Havlicek: Would you like to do methodology?

Chloe Colliver: Of course. We use a mixture of social listening analytics, which looks at public social media data from Facebook, Twitter, YouTube, the major platforms that we all know of, but we also do work that looks at the smaller, alternative technology platforms that are often used to mobilise or plan information operations. That would include chat forums and closed chat apps like Telegram or occasionally WhatsApp.

Finally, we do network mapping to look for inauthentic networks acting at scale where we have access to that data. It is a mixture of qualitative and quantitative research that looks for anomalies in the datasets and information around election.

Sasha Havlicek: Combined with that, we also do an in-depth monitoring of media and broadcasting. We have been looking of course at Russian state media but increasingly also at other media operations from Hungary, from Italy and from Poland. That combined analysis we have applied now across six countries in the lead-up to the European elections.

It may be worth just saying a little bit about what we see in terms of the evolution of the trends in disinformation across this recent period, three years. Many people have been looking, I think, for what happened in 2016. They have been looking for the same actors and the same tactics. That picture in our minds has largely evolved, or at least it is much more complex, as we have dug into what has been going on across these countries.

In terms of the actors, of course much focus has been on hostile state actor interference and influence operations. In reality, the picture is much



HOUSE OF COMMONS

more complex in terms of actors. What we have seen is quite considerable efforts made by transnational non-state actors combined with the operations of both domestic political and domestic non-state extreme and populist actors. That presents a wholly new set of challenges. It is increasingly hard to identify the line between foreign state and domestic activity—between, if you like, legitimate and illegitimate activity. Again, it is important to understand that we are looking at a complex set of actors.

In terms of tactics, we have seen an evolution of the tactics from the obvious fakery of 2016—fakery in terms of content itself but also fakery in terms of distribution. That is not to say that we are not seeing that type of activity. We have, in fact, identified a whole range of inauthentic networked operations across every one of the markets that we were looking at. These were the major European markets in the lead-up to this European parliamentary election.

It is to say that what we are seeing is a more complexified picture where we have identified a shift from traditional information warfare and outright fake news, distributed through botnets or seeming botnets, to a kind of narrative competition where you see the use of legitimate content, often from legitimate sources, being used in a manipulated way out of context to paint a picture.

Those pictures are being painted around key wedge political issues, including of course issues like migration, which have particularly divisively utilised and leveraged by populist and far right groups, and issues like family values versus progressive values. There has been a concentrated effort looking at, for instance, the denigration of LGBT efforts. There is a great deal of harassment in relation to women, a kind of anti-feminist stream that we have seen arise across these elections in a number of countries, but we also see now increasing activity around the issue of climate and climate denial. I think we will start to see more of that type of engagement.

Again, the actors here have been manifold. There are certainly operations that are aligned with American special interest groups. We see investments from those interest groups—as we have seen in the past, in fact—in relation both to financial and organisational and operational support to those types of operations.

Just lastly, in terms of the targets, we have all been very heavily centred on these operations as they apply to influencing electoral outcomes. In actual fact, what we see is investment in long-term information operations around issue sets with a view to, if you like, shifting cultural norms and mindsets in a way that would be supportive of longer-term political objectives. We see these operations happen in a much more opportunistic way. Events, for instance, like the Notre Dame fire were jumped on and leveraged to further a kind of polarisation narrative



around Muslims versus Western civilisation, something that we have seen on a number of occasions.

I should say that there are a number of very dangerous, extreme ideas and concepts that have successfully been mainstreamed from fringe groups into the political space that are worth noting, for instance concepts like “remigration”, which is essentially a call for ethnic cleansing by another name. This is a concept that is particularly popular within identitarian circles across Europe, born out of a conspiracy theory around ‘the great replacement’ which inspired the Christchurch attacker.

Concepts like this, which have been campaigned on in the alt-right circles of the alt-tech nether regions of the internet, have in many ways, we have seen now, broken through into the mainstream with, for instance, the AfD in Germany, the second major political party in Germany, now using the term “remigration” in its electoral campaign sloganeering quite publicly around this. The term has been seen to be taken up across social media channels in a number of European countries. These sorts of developments, I think, are important to watch out for.

Q143 Julian Knight: Just a couple of questions in terms of the evidence that you have looked at on this move away from what you call “information warfare” to “narrative competition”. First, what impact do you think that has had on the results? Secondly, what does this mean for content regulation of online platforms?

Sasha Havlicek: Drawing a linkage between these sorts of information operations and assessing their impact on electoral outcomes is extremely difficult and I do not think that any researcher has the data available to be able to make that connection, but I would say that what we are able to identify very clearly is where certain concepts start to become mainstreamed. There are technologies available.

We work with MIT on a tool, the Media Cloud, which is now enabling us to track and trace certain types of concepts and political language across the media ecosystem, across the mainstream of the media ecosystem but also into the fringes. We are able to start to see the point at which these ideas start to build momentum and start to dominate the political discussion.

I should say that we have not come to the end of the analysis that we are doing now based on the data that we have collected. One of the things that we will have over the coming weeks is a clearer picture on the extent to which, for instance, issues that populist parties but also extreme groups mobilised around ended up dominating not just social media channels but also wider mainstream media channels and how that related in the end to the polling data that was being collected across these countries. I think once we can compare and contrast those data sets we will have a much better sense of the correlations.

Q144 Julian Knight: Just before we turn to the second part of the question,



soon you will be able to basically track the proliferation of these ideas in the body politic and then overlay that with the polling data to show, effectively—say a party has an anti-immigration message—the strengthening of that as polling day approaches and those parties going up like that. Is it fair to say that there will be real, strong empirical evidence to suggest that there was maybe substantial influence on the results themselves and you will be able to draw that parallel?

Sasha Havlicek: Yes. I should say that already now we do see a substantial divergence in terms of polling data and the issue sets that dominated, in many senses, the social media discourse. I think it is important that we do not see the social media universe as a direct reflection of reality.

For instance, we saw in many countries almost hyperactive activity rates but also engagement rates of populist parties on Facebook, for instance, in relation to all other parties on the subject of the European parliamentary elections. We saw extraordinarily disproportionate activity of those parties vis-à-vis all others and yet in many of those contexts of course that did not, in the end, come to have an impact on the election outcomes themselves. For instance, the AfD did poorly, less well than was expected in a German context. It does not necessarily translate into the real world. Again, Twitter does not necessarily reflect the real world entirely.

Julian Knight: I hope it does not, actually.

Sasha Havlicek: I hope it does not, but we will get a picture of the extent to which that is or is not the case.

Q145 **Julian Knight:** In terms of the move to narrative competition that you very ably outlined for us, what does it actually mean for content regulation in online platforms?

Sasha Havlicek: It makes it much harder. We have advocated for some time a need to shift from content moderation approaches in policy, which look at removing primarily illegal but problematic content, towards a policy approach that takes into account the technological architecture of these platforms and specifically the ways in which that technological architecture may amplify, in an inorganic way, certain types of messaging. This is extremely important because the type of content that we are seeing many not, in fact, in itself, be problematic.

We desperately need now a shift towards a focus on problematic behaviours: that is to say behaviours in terms of networked inorganic amplification, for instance. That is the first thing. The second thing would be—

Q146 **Julian Knight:** Sorry, “networked inorganic amplification”? Is that bots?

Sasha Havlicek: It could be a mixture of bots, cyborgs, sockpuppet accounts and so on, but essentially the system being gamed.



Q147 **Julian Knight:** Okay, I get you.

Sasha Havlicek: I should say, in terms of that complexity of the picture, that one of the reasons why I think we are finding it harder to identify these very large botnets in the way that we may have been able to previously is that the approach to that kind of inorganic activity has shifted. It is now easier to buy networks of existing accounts that may be less obvious in terms of being able to be spotted by the companies or indeed by researchers, and they are very cheap.

Jigsaw did a piece of research that I think is quite important. They demonstrated that you could in fact buy a botnet in support of a pro-Stalinist campaign for almost no money and it would have a great impact. These sorts of tactics will likely be being deployed and it may be one of the reasons that it is harder and harder for researchers to identify this.

In terms of the focus for policy, it is absolutely vital that we look at these structural challenges. First, we need to have a better understanding of algorithmic output. This is not about algorithmic transparency. No one would know what an algorithm meant if it hit them in the head. This is really about having access to data to be able to do third-party review of algorithmic outcomes. How are you receiving information differently to you or to me? What is the impact, from a public health standpoint, of the way in which that is happening? That is number one.

The second thing, of course, is data and the way in which data is being used to target us. Of course that is being done for commercial purposes but in the context of political processes and mobilisation I think we have to have a very different set of criteria and rules. That is not currently the case and represents a set of problems. That is where I believe the focus of policy and indeed regulation needs to go. Some of this is addressed in the Online Harms White Paper, but not comprehensively enough, I think, and I would hope that we would see that process shift a little bit further away from content moderation to these structural issues.

Q148 **Julian Knight:** Have you been in touch with the likes of Facebook, Twitter and so on about your findings? In your report you conclude the tech companies are “failing to fulfil their many promises to safeguard the integrity of elections”. If you were in touch, what did they say?

Sasha Havlicek: We have been, on a weekly basis, providing them with data on any inauthentic, inorganic activity that we have been identifying across these platforms. We have had some response from Twitter. We are yet to have that conversation with Facebook. We would like to see much more responsiveness—

Q149 **Julian Knight:** But you are telling them? You are telling Facebook what you are doing?

Sasha Havlicek: Correct, yes.

Q150 **Julian Knight:** They are basically just ignoring what you are saying at



HOUSE OF COMMONS

the moment—is that fair?

Chloe Colliver: That is correct. We have been trying to measure their enforcement of the EU code of practice on disinformation throughout this election, which is obviously a voluntary code of practice, self-regulatory, and we would say that in large part that has not been enforced properly or fully by the platforms.

For example, one of the voluntary commitments they made there is around integrity of services. That includes being transparent around how they detect inauthentic accounts, when they find them, when they remove them and the potential reach or impact of those kinds of networks and accounts. That is not something that we have seen fulfilled through this election.

Secondly, on the advertising point that I know was spoken about in the previous session, there were a number of false positives and false negatives and a very difficult to use API for researchers to understand political advertising. We saw in the UK but also elsewhere adverts that contained misinformation around the election targeted at political issues and political individuals. We did try to measure across those commitments whether they were enforcing them of their own accord in a substantial way and for many of those they did not appear to do so.

Q151 **Julian Knight:** Just to clarify, you are telling Facebook—let us focus on them for a second—that they are potentially in breach and they are completely ignoring what you are saying at present? You are sending them all this information and they are sitting on their hands and doing nothing? Is that fair?

Chloe Colliver: We received one reply from Facebook for one of the particular networks that we flagged to them, just so they could confirm what the correct information was we were sending, but we did not hear back from them on any action that was taken on that.

Q152 **Julian Knight:** How many communications have you had with them?

Sasha Havlicek: We contacted them, in the last month before the election, four times, sending weekly stores of content that we were finding.

Q153 **Julian Knight:** You have had one communication. In the month leading up to the election you sent weekly updates. You are obviously an institution that people know about, that they will know about and so on. They acknowledged and checked one bit of data and you have heard nothing since the election? That is it?

Chloe Colliver: That is correct.

Q154 **Julian Knight:** Despite the fact that you have told them that they are in breach?



Sasha Havlicek: What we do not know is the extent to which they started to remove some of that content. We do know a campaign organisation called Avaaz provided them with a big store of data on essentially accounts that were promoting hate speech across Europe. They did take action on part of that network, but not all of it.

Q155 **Chair:** Can I just ask, when you were reporting to Facebook were you reporting not just on content that falls foul of the regulations but also on, potentially, networks of inauthentic accounts?

Chloe Colliver: What we flagged to them as a priority were networks of what we believed to be inauthentic accounts. Obviously, researchers now face an enormous lack of data to do that research and our findings cannot be 100% certain. Facebook have access to a trove of data on those accounts and networks that they would be able to then investigate and verify. We did explicitly ask them to let us know if any and what action was taken on those networks that we send them through and we did not receive a reply.

Sasha Havlicek: We do define “malign information operations” as operations that are either illegal content—for instance, there is an enormous amount of illegal hate speech, harassment, defamation and the like—but also deceptive content or distortive activity: networked operations, for instance. We will classify the operations and the accounts in that way and provide that data to them in that way.

Q156 **Chair:** In your report you noted that five of the top 10 accounts mentioning the Brexit Party on Twitter were producing over 144 tweets per day, indicating, in the words of your report, “bot-like activity”. Could you tell us a little bit more about this and the nature of the content that these potential bots were sharing?

Chloe Colliver: Yes, of course. It is safe to say that we were surprised at how explicit some of the accounts we found promoting different UK parties and also attacking different UK parties on Twitter were in terms of their bot-like activity. It is actually quite rare for us now to see such explicit, almost certainly bot accounts on Twitter. They have done a much better job at removing a lot of those explicit bot accounts across the board.

However, in this instance what we did was we looked at the Twitter handles of all the UK political parties taking part in the European elections to see the 10 accounts that were most active either in mentioning, retweeting or replying to the political parties’ Twitter handles. You get the network of accounts around each party.

I believe 42% of all those accounts that we looked at for the parties gave strong indicators of bot-like activity. That is a mixture of looking at their level of activity and how often they tweet, but also signs of anonymity such as whether they have a believable name and picture and whether



HOUSE OF COMMONS

they post content just from one kind of source continually or whether they have a varied kind of activity.

It is not an exact science, hence the language of “bot-like activity”, but it was a very high level of probably inauthentic behaviour both attacking and supporting political parties. We saw most of the accounts most active around the Conservative Party Twitter handle were attacking the Conservative Party, whereas for other parties, for example, the Brexit Party, we saw that those bot-like accounts were promoting the Brexit Party. It was a mixture of bot-like accounts being used to denigrate opposition parties and support certain parties.

Q157 **Chair:** For the bot-like accounts that were particularly active in promoting Brexit Party content, was there a particular type of content they tended to focus on or was it a range of issues?

Chloe Colliver: A lot of the content was in reproducing official Brexit Party content. There was not one particular issue area; it was attacking a range of parties. They attacked Change UK, they attacked the Conservative Party, some attacked the Labour Party. It was quite a broad range and it did not appear to us there were obvious signs that those accounts were co-ordinated together.

Q158 **Chair:** Do you think the level of bot-like activity around content from the Brexit Party was greater than it was for other political parties in the UK or was it broadly similar?

Chloe Colliver: Within the top 10 accounts that we looked at for each party, the Brexit Party had the most probable bots within that top 10 account list, but we did not look more broadly at the bigger networks around each party.

Q159 **Ian C. Lucas:** Just one point. I had a false statement made about me within a Facebook group that was presented to me. When Facebook were presented with the falsity, they contacted people relating to the post but they refused to take the post down. My understanding of Facebook’s general position is that they will not remove false posts. Is that correct?

Chloe Colliver: Facebook has a very unclear policy around disinformation in general. For example, I am sure you are all aware of the Nancy Pelosi doctored video, which they refused to remove under the grounds that it was relevant to political debate, whereas YouTube, for example, did remove copies of that video. There is no clear policy from Facebook on when it will act on disinformation and when it will not.

The regulation around the Online Harms White Paper could do well to draw more concrete lines on when something might be harmful and it would be necessary for them to take action on that. It is within their terms of service, their community guidelines. Defamation as a nationally illegal concept within the UK would fall within their community standards but there are many examples where we see that not acted on.



Q160 **Chair:** Philip Gradwell, we were talking in the session with the Electoral Commission about the way in which tools like PayPal can be used to process transactions into political parties that may be impermissible. We just heard a bit about bot activity in promoting political parties' content. To what extent do you think we should be concerned about these sorts of tools being used by inauthentic actors to process money into political campaigns?

Philip Gradwell: Should I give a little bit of context about Chainalysis, to lay out the perspective from which I am speaking? Chainalysis provides software for investigations and compliance for cryptocurrency. We provide that to law enforcement if they want to, say, track payments out from ransomware and for cryptocurrency exchanges so that they can conduct AML on the transactions that they send and receive.

Q161 **Chair:** Sorry, AML being—

Philip Gradwell: Anti-money laundering. From our perspective, the blockchain is very transparent. All transactions are recorded and that record is there permanently. However, those transactions are pseudo-anonymous. There is a string of letters and numbers, an address, which represents an individual rather than an individual's name or indeed the service, say, in an exchange or a merchant service payment processor that sent that transaction. This means that you can trace the flow of transactions with a very high degree of confidence and transparency on the data, but to link that to a real world entity is harder.

What Chainalysis does for the services that operate on the blockchain is provide that mapping. We do not contain any sort of personally identifiable information but we focus on the businesses, which are often where most individuals will interact. For example, they go to an exchange and they transfer their pounds and they buy some Bitcoin. That is the context of the perspective that I bring.

We have not seen a large amount of cryptocurrency flowing into political donations. Most of that will have happened in the US. In the UK it is not something we have come across. There are flows of donations often to far right groups. There, there has been a bit more evidence. It is probably a trend that we will see in the future but so far it has not been significant.

Q162 **Chair:** Just so we are clear for the record, by "cryptocurrencies" you are talking about the trading of actual cryptocurrencies rather than just micro-financial transactions processed from people's real bank accounts into—

Philip Gradwell: Yes, for cryptocurrencies specifically.

Q163 **Chair:** What do you think is the vulnerability of this? We have raised this with the American Electoral Commissioner and she was very concerned that the prospect of Facebook having its own cryptocurrency could create a whole generation of new problems for monitoring political donations



HOUSE OF COMMONS

and financial support for campaigns.

Philip Gradwell: Facebook released their white paper on their new cryptocurrency just before this Committee came into session. I cannot speak on the specifics of that, but they have a very large user base and that will open up cryptocurrency to a very large number of new people. There are some benefits of increasing financial inclusion but it also does increase, if you like, the financial inclusion of bad actors and does give them that scope. It is definitely a risk that needs to be mitigated.

Our experience of working with cryptocurrency exchanges is that because of the transparency of the blockchain, if you do put in anti-money laundering systems you can trace transactions. For example, say someone were to split a set of donations up into smaller amounts and then send them individually; you could actually trace that back to a common wallet. You start to get techniques because of the transparency of the data that are not available in traditional financing. However, if you do not take action then those risks are definitely, inevitably going to be there.

Q164 **Chair:** Do you think a political party could put in place anti-money laundering practices that would help it identify the likely original source of cryptocurrency payments?

Philip Gradwell: it is definitely possible and feasible. Whether that responsibility sits with the political party or, say, a payment processor who might operate on behalf of them is another question.

Q165 **Chair:** One of the questions we were asking of the Electoral Commission was about whether bots were processing transactions into a political party using PayPal. Do you think blockchain technology could be utilised to make or help make multiple micropayments into a political party?

Philip Gradwell: Yes, definitely. That may be more possible on a blockchain because it is easier to programme the transactions, but at the same time it is then also easier to trace those transactions back to a common source.

Q166 **Chair:** You have to know that is who you are looking for, though.

Philip Gradwell: Yes. We spend an awful lot of our time trying to understand the obfuscation patterns that people generate. There is a constant cat and mouse game but it is not one we feel like we are losing.

Q167 **Chair:** We discussed with the Electoral Commission the issue of the Brexit Party and the possibility that they could have received payments processed by bots. If that had happened, would it be possible for an investigator to go in and look to trace those transactions back to a common source if it was from a bot?

Philip Gradwell: If it was a set of blockchain transactions, that would be possible.



Q168 **Chair:** Are you aware of blockchain technology having been used anywhere in the world to try to facilitate the processing of micropayments to political parties?

Philip Gradwell: Not to political parties. There have been some US politicians who have been accepting cryptocurrencies. The scale of those payments is not clear. Our understanding is that when they have raised money through those means they have tried to do it in a compliant way. I don't think there has been evidence yet of people trying to use cryptocurrencies to make non-permissible payments.

Q169 **Chair:** What we are interested in now is: is this a technology we should be taking greater interest in? Is it possible for people who may wish to hide the level of donations they are making, to make impermissible donations or even to launder money into a campaign to hypothetically use this sort of technology to try to do that?

Philip Gradwell: Absolutely. There is that risk. It can be mitigated against, but if it is not then it definitely can be abused. The experience from darknet markets, say, is that there we see cryptocurrencies being used as a payment conduit or payment channel for illegal businesses. Now law enforcement is defending against it, that problem has not gone away but it is more manageable. Definitely those risks have been replicated in other sectors and there has had to be a response.

Q170 **Chair:** When you say that there are things we can do to mitigate that, what recommendations would you make to the Committee of ways in which we could mitigate those risks?

Philip Gradwell: One of the core challenges with cryptocurrency transactions is that there is not an identity that is associated with that payment, and so KYC does become very important.

Q171 **Chair:** KYC?

Philip Gradwell: Know your customer. When someone makes a deposit or a donation, you get some verifiable identity information. That is information that anyone doing the blockchain analytics will not see. It is an important part of it. But then I think you do also need to do that blockchain analytics. In the same way that you might ask, "What was the source of these funds?" you are asking exactly the same question when it comes to cryptocurrency.

Q172 **Chair:** In some ways, the two things you have identified—knowing the source of the funds and knowing the customer—are the two principal ways you would try to mitigate against abuse of blockchain?

Philip Gradwell: Yes.

Chair: They are two things that the Brexit Party, for example, was not doing in terms of the way they were processing payments, it would seem.

Q173 **Ian C. Lucas:** What current rights do we have to access the chain so that we can investigate sources of finance?



HOUSE OF COMMONS

Philip Gradwell: You have the complete right. Anyone can download the blockchain and look at it.

Q174 **Ian C. Lucas:** If I download it, I haven't a clue what the numbers are.

Philip Gradwell: That is the thing. The data is unstructured and so there is a job to structure it. I guess that is the reason why my company does exist: to do that.

Q175 **Ian C. Lucas:** This should not be seen as you doing an advert but if I wanted to investigate blockchain, would it be possible for you as an individual to investigate and give me a report on who these people are?

Philip Gradwell: It is not possible to give a report on who they are because there is none of this personally identifiable information on the blockchain, but it is possible to trace back the source of funds to other addresses.

Q176 **Ian C. Lucas:** Which are numbers.

Philip Gradwell: Which are numbers. There are publicly available datasets that do map some of those addresses back, often to the services—the exchanges or the businesses that operate on the blockchain—and there are a number of public tools. Then obviously as a company we then add more information to that.

Q177 **Ian C. Lucas:** Can people like the Electoral Commission or the police actually identify the source of the blockchain?

Philip Gradwell: They can identify the source of funds. What will often happen is they will trace it back to an exchange, for example, where people transferred their sterling into Bitcoin, and that then gives them an entity that they can then go and ask, "What was the KYC information of the person who made this specific transaction?"

Q178 **Ian C. Lucas:** Do you know if they have the legal powers to do that at the moment?

Philip Gradwell: There are obviously jurisdictional issues. If you are the UK police you can ask a UK-registered entity. One of the challenges in cryptocurrencies is that it is easy to send payments globally and so if you were to trace a transaction back to a non-UK exchange you would then have jurisdictional issues.

Q179 **Ian C. Lucas:** If the police, for example, followed a chain and it led to Russia, would they be able to obtain the identity of the source?

Philip Gradwell: I cannot speak to the ability of the police to do that type of work. I would say that the UK police forces are already working on this type of problem in cryptocurrency payments, tracing it back to different exchanges—

Ian C. Lucas: That would really depend on the Russians, would it not, giving the information? Thanks.



HOUSE OF COMMONS

Q180 Chair: I just want to bring in Tom Packalén at this point; he has been waiting very patiently. You are Chairman of Utopia Analytics and you work for the largest social media platform in Finland to help them moderate content. Many of the issues we have been talking about are identifying harmful content that should be acted against by the major tech platforms, who do not often do it as efficiently as we would like at all. I wonder if you could explain a little bit about the technology that has been developed by Utopia and some of the insights you have gained from the application of that technology.

Tom Packalén: Thank you. My background is from the police. I was Chief Inspector at Helsinki Police Department before I joined Parliament in 2011. This company was founded in 2014, Utopia Analytics, and we are specialised in text AI. Behind our technology is machine learning studies and research in Helsinki University and other universities. My CEO and co-founder of Utopia Analytics, Mari-Sanna Paukkeri, had her first thesis in her PhD about language independent text analytics.

We have a different approach to the traditional approach to analysing text. We analyse all languages, all dialects. The traditional way text is analysed is based on studies made in the English language, the easiest language for a machine to learn and understand. The Finnish language is the opposite. It is one of the most difficult languages in the world for a machine to understand. The way this technology was built, it was built to handle Finnish language but at the same time we can handle all other languages because this approach is totally different to the traditional way, NLP, natural language processing. This is the basis of our technology.

A Utopia AI moderator tool, we announced it in 2016 and we can do in milliseconds all the comments. Of course humans have to make the decisions about what is good and what is bad. We do not make these decisions in our company. It is just a tool, but we can give answers in milliseconds. Is this proper or is it against the policy of that forum?

Most of the biggest Finnish news agencies and platforms use it, but also big chatbots like "children's Facebook", Momio in Denmark, that has over 1 million messages a day. They use this. Because it is children, if there is grooming it sends a message that this is not acceptable. If there is self-harming, it sends the message so that if you want you can call an adult in your country. We do this Momio work in nine countries. It is a very advanced and powerful tool. With the numbers of comments in social media, it is impossible to handle this number. It is billions. If you do not have working artificial intelligence there it is impossible to handle this amount of comments.

Q181 Chair: How quickly can the tool respond? If someone posted content on their social media account that was in breach of hate speech rules or other forms of harmful content, how quickly could the tool identify that content?



HOUSE OF COMMONS

Tom Packalén: Like how long it took to build the tool, or—

Chair: Once the tool has been built.

Tom Packalén: It is milliseconds. It is a fraction of a second. It depends how long the distance how fast it goes, pretty much. If it is a different continent it will take a few more milliseconds, but it is fast. It is real-time.

Q182 **Chair:** How do you think the tool that your company has developed compares to other content moderation tools used on the major social media platforms like Facebook or YouTube?

Tom Packalén: Of course I do not know all the tools but we pretty much know the technology that is behind these different companies and of course we are very proud of our tool. It is very powerful.

Facebook have said it might take another five or 10 years before the technology is there. It is a very strange situation. Why they said this, I do not know.

Q183 **Chair:** You believe that the technology exists now to provide effective content moderation on platforms like Facebook?

Tom Packalén: In 2016 our company offered Facebook help to do this moderation of their content but they were not interested. In 2018, when in Sri Lanka there was violence between the Hindu and Muslim population and there were people burned alive, we offered to build a model for the Sinhalese language in two weeks for them to help in this case. On 21 April last year, over 250 people were killed in this violence. Also at that time they were not interested in our help.

Q184 **Chair:** They were not interested in your help?

Tom Packalén: No.

Q185 **Chair:** Did they express an interest in the technology at all? Did they think it was technology that could have been used on their systems?

Tom Packalén: In 2016 they said it was difficult to work with a third party and it would be acquisition if they do co-operation but they are building these things by themselves. They were not too interested in this issue.

Q186 **Chair:** They said they would only work with a company like yours if they could acquire it? They would not work with a third-party provider?

Tom Packalén: Yes. This was in 2016. I really do not know. This is a question one must ask Facebook, why they did not want to go further or even test, because we can build for free in two weeks a model that could help them. It was a surprise for us too.

Q187 **Chair:** Yes. What is interesting is that Facebook are saying it is going to take five or 10 years to build the technology to do this but you are saying



there is technology that exists now that could help. It does beg the question as to why that has not been used, or considered, even.

Tom Packalén: This is the question. Of course we do not know and we cannot say for Facebook why, but I could imagine that also this is not their core business. If there are tools like this it will take 5% of all the comments away and it is 5% less advertising, and money comes to Facebook from their advertising. It might be the one reason, or they just have not had the capabilities but even if they do not have the capabilities they know that there are capabilities in the world.

Q188 **Chair:** It would seem as well, from what you are saying of the case in Sri Lanka, that you can build a model for this technology to operate in a new country, in a different language, very quickly.

Tom Packalén: In two weeks, we promised them that it would be built. In two working weeks, we would build a working, fully functional model for them for Sinhalese.

Q189 **Ian C. Lucas:** I had a conversation with another gentleman. His evidence to me about automated systems was that he was running a company that sounded a bit like yours. It is right, is it not, that there are other businesses that run this same type of system?

Tom Packalén: There are a lot of AI companies who do text analytics. The difference for us is the language-independency that we have. We can do all languages in the world and all dialects. It is also important to understand that social media language is totally different to the formal language on which NLP is based. There could be other networks and other algorithms over top of that, but it is made for formal language and dictionary words. In social media, people use words with totally different meanings. It is very complex for these NLP technologies to handle.

Q190 **Ian C. Lucas:** Yes, but my basic point is that there are a number of companies who do this.

Tom Packalén: Yes, indeed.

Q191 **Ian C. Lucas:** Can you clarify for me how you designate whether particular content should be removed? Would that be, for example, decided by Facebook, what the rules were that they were going to apply?

Tom Packalén: This is an excellent question. In our company, our policy is that we do not make rules. We do not decide what is right or wrong. That is too much power for any AI company to have, at least in my opinion. We just provide a tool and the company make the policy of what is right and what is wrong. We learn from the data what the moderation policy has been before and our machine understands semantics or bigger meanings of the content, not just words. The traditional way is just, "This word, this word, it is bad"; an enormous number of rules. Our machine learns just from the data what the policy is, what is acceptable and what is not.



Q192 **Chair:** I wonder if I could ask Sasha and Chloe. Do you think this technology could have a role in identifying disinformation campaigns in real time as they are being created on social media platforms?

Sasha Havlicek: Yes, absolutely, and actually we have worked with partners on NLP systems to be able to identify extremist content. I do think that there is great potential in this type of approach and I do think that the companies have in fact said that they are heading in the direction of automated systems to identify hate speech. They certainly use those systems in relation to, for instance, terrorist content and violent extremist content already. According to their own transparency reports, they remove that type of content 99% of the time through these automated systems, so the systems do exist in relation to certain problems but are not applied across the board.

I do think it does depend on the priorities the companies set in terms of what they are really looking at and what they are trying to solve for, and part of that is also a question of where Government pressure is.

Chloe Colliver: I would just add that I do think an increasing trend is image and video-based disinformation, for which obviously that kind of tool would not necessarily be fit for purpose. Equally, a few small studies have looked at particular disinformation campaigns or elections and seen that the trend is towards using legitimate, trusted media but misrepresenting it or taking it out of context, these kinds of subtler approaches to disinformation that necessarily would not be flagged as something outright.

Sasha Havlicek: Again, a content-only approach will not really cut it. We do need to look at behaviours in terms of inauthentic amplification, for instance, but also these wider challenges around algorithmic bias in amplification.

Q193 **Chair:** Tom, do you want to come in on that?

Tom Packalén: If I may. Facebook have said that they can handle over 95% of terrorist messages involving jihadism or whatever, but it is mostly, like you mentioned, about pictures and videos, and they are much easier to handle than text. Text is much more complex. With hate speech, they are promising something like 35%. This is the complexity of text. It is like unstructured data when it is not done by an NLP. It is much more difficult to handle.

Q194 **Chair:** One of the recurring debates in this is about whether the technology enables more effective moderation or not. Often the platforms seem to suggest that the technology does not enable it but it would seem that there are technological solutions to some of the problems, even though the problems around image and video are very different.

Chloe Colliver: I would flag briefly that just before the European elections in Germany, Twitter implemented a new, slightly more automated and faster system for removing accounts that were reported



to be spreading disinformation. That system was manipulated and gamed by certain far right activists who were able to use that system to report legitimate political and media activists, who were then removed. I do think there are huge warning signs around the application of this without real testing.

Sasha Havlicek: Secondly, just to remind ourselves of what type of content we are talking about, often this is very nuanced ideological content. There needs to be a great deal more emphasis on expert-driven training-up of these systems. We have just come across, for instance, a whole lot of older Islamist extremist content still sitting up there and not being addressed. Part of it is the ideological understanding of this type of content, which requires partnerships with academic institutions and civil society organisations.

Q195 **Chair:** Do you think this sort of technology can facilitate not just content moderation but also the identification of inauthentic activity on the platform as well? A network of inauthentic accounts might be using similar messaging and therefore there could be something very specific to a particular campaign launch on a particular day. Do you think this sort of technology would make it easier to identify some of those networks?

Chloe Colliver: There are certainly technologies that would help with that. The major issue at the moment is data access. I think the technologies are out there that we could use if we had access to some of that data, but currently that is not possible for most platforms.

Tom Packalén: One words about bots. We probably could recognise bots, if it is made by bots. The distribution is different than when it is done by a human. It is probably doable, but we need specialists to understand which are probably bots and which are not. We would just search this distribution and these kinds of things, but it would be very interesting.

Q196 **Chair:** What you were saying earlier on that was that the bot technology has become more sophisticated, but looking at the sorts of problems we were looking at in 2016, if bots were using unusual formulations of language that might suggest a person was not doing it in their native language, this sort of technology would probably help to identify common mistakes, common ways.

Sasha Havlicek: Absolutely. The intersection of those different technologies applied at the same time.

I should say that just because we are seeing an evolution towards more complex means of disinformation does not mean that we do not still find quite obvious inorganic activity—botnets, cyborg nets and so on. We have found those.

The companies did make very strong statements and commitments in relation to dealing with those types of illicit behaviours on their platforms and that still is not being done at scale. If we were able to find them, it



HOUSE OF COMMONS

means that this is probably the tip of the iceberg. We had a research team across these six European countries but not beyond, quite small, so I would say there is still quite a major problem in terms of these illicit behaviours.

Chloe Colliver: There is also a consideration here for using these technologies to at least do some of the preliminary work on identifying content moderation issues, partly because the individuals who are currently outsourced and tasked to do content moderation for these companies are faced with enormous trauma. They are given about eight seconds, on average, to look at a piece of content and make a decision on whether that is against or within the terms of service of a company.

Often it is violent content, sexual content, and a number of studies have shown that there is an enormous amount of PTSD and some suicidal issues among content moderators who are hired and outsourced by these companies. I do think that any way to reduce the burden on individuals to have to look at rafts of this kind of content would be helpful.

Q197 **Chair:** Yes. Technology could sift out the obvious stuff and then the moderators would only need on to focus on the—

Chloe Colliver: Or at least to triage it and prioritise what looks like it is most likely to be against the terms of service.

Sasha Havlicek: I would say though that the focus of Government on specifically foreign interference, foreign state interference, and on elections alone means that the institutions set up to look at this kind of inorganic behaviour and information operations writ large and indeed the companies themselves have a fairly limited scope. I think that is where the problems will lie long-term. We need to be looking across these actors, their tactics and these different targets that we see now in play.

Q198 **Chair:** These issues again seem to reinforce the recommendation that there should be regulatory statutory powers, the ability to go and audit companies to see if they are using systems that would be considered to be best in class or if there is technology they could deploy but they are not doing it, and therefore if that is a contributing factor to their poor compliance with content moderation and acting against hate speech.

Sasha Havlicek: Correct. Third-party review of that data is absolutely necessary right now. We cannot see behind that curtain and neither can Government.

Q199 **Chair:** Yes. Just finally from me, for Philip: I appreciate as you say that the Facebook white paper has only just been published on their cryptocurrency but again, would you have concerns if a currency launched by Facebook was run in the same way everything else on Facebook was run, which is behind a massive wall? Would that give us a big cause for concern?



HOUSE OF COMMONS

Philip Gradwell: Yes, that is probably fair to say. Without transparency on how those decisions are made, you are now making decisions about flows of money in addition to flows of content and so on.

Q200 **Chair:** Indeed, it would seem that if it did not have that, Facebook would effectively just bypass all the global financial regulations and all the anti-money laundering legislation because they would have created the perfect money launderer's product.

Philip Gradwell: Yes—if they were operating without the normal financial regulations, then of course.

Chair: It has been a fascinating discussion. Thank you all very much for your evidence this afternoon.