**NOTE OF MEETING WITH FACEBOOK**

**Date: Wednesday 20 September 2017**

**Time: 13:00 - 14:30**

**Location: Facebook offices, 2 Stephen St, London, W1T 1AN**

**Present:**

* + Simon Milner (SM), Policy Director, UK, Middle East and Africa, *Facebook*
  + Sean Evins (SE). Head of Europe, the Middle East and Africa Government Outreach, *Facebook*
  + Emma Collins (EC), UK Public Policy Manager, *Facebook*
  + Lord (Paul) Bew (PB), Chair, *Committee on Standards in Public Life*
  + Jane Ramsey (JR), Member, *Committee on Standards in Public Life*
  + Lesley Bainsfair (LB), Secretariat, *Committee on Standards in Public Life*
  + Maggie O’Boyle (MO’B), Secretariat, *Committee on Standards in Public Life*
  + Dee Goddard (DG), Secretariat, *Committee on Standards in Public Life*

PB: We are very grateful to you. PM asked us to look into these issues of intimidation - arguably for the first time, in some people’s minds not for the first time, intimidation of MPs happened during the election [June 2017] and Social Media Platforms were a part of that. We promised to produce a report for her by Christmas. We have taken quite a lot of evidence thus far, indeed we did meet the parties in a public session towards the end of last week.

PB: If I could begin by asking just a basic question, what do you think the responsibility of Social Media platforms is in relation to abusive/threatening messages. You’re probably aware I’d imagine in your world everybody looked at the recent FT piece which was arguing that basically some way or another you should be taking more responsibility. We understand this is not a simple matter, but what is your reaction to the FT piece and generally to this problem of responsibility.

SM: Sure, I’ll kick off, provide a broad perspective. To set the scene, so I am policy director for Facebook in the UK and several other countries in Europe, Middle East and Africa. I have been in the company for about 5 ½ years. I would say of all the policy issues that I have to engage in, it is the safety of people who are using our service which is the most important, the one that I get asked the most questions on, the one we do most work on. Because we know that it’s the thing that people frankly care most about. When things go wrong, on a platform like Facebook, when speech, particularly in this space where political speech can often get quite heated, when it goes beyond heated into abusive and threatening, it’s absolutely an area we think a lot about and we are really trying very hard to get things right. A lot of what I do is focused on young people and vulnerable individuals if you like. I’ve been a Member of the UK Council for Child Internet Safety which is this government convened body, that’s looked at that really since its inception. Certainly I’ve spent a lot of my time on that. In many ways we have brought what we learnt from that area to the issue of political representatives and would be political representatives if you like, candidates and elections and others, and trying to bring that learning but we are not as far advanced on that issue as we are on the safety of young people.

But the framework is still the same - so it’s about clear policies, what are you allowed to say or allowed to do and what are you not allowed to do, and then it is about the tools you provide for people to protect themselves, and so how do you protect yourself from somebody bullying you or trying to infringe your rights or whatever. The tools we provide for you to tell us about things, so the reporting tools are extremely important, the tools we provide for people managing a page. So a lot of work around the tools so kind of ‘Designing in Safety’. And then ensuring we have got expertise and people to handle reports when you raise issues with us.

We’ve got more than 2 billion people using Facebook pretty much every week.

We get millions of reports every week about things that are happening on Facebook and quite a lot of them are, you know, [ ] there is a lot of noise as you might expect, but a lot of them are people who are genuinely concerned about behaviour towards them or towards others on the service. And that is not surprising.

We are a country of 65m people, how many crimes are committed every week in the UK. People need to know they can report it and act on it. We now have about 4,500 people who work in our community operations team, those are the people who handle reports and as it were look at the report, look at the issues, look directly at the content or the account or the page or whatever it is that’s at issue, and then look at our policies, and say ok is it falling foul of policies or not. If it is what are we going to do about it. Take down the content, take down the account, take down the page. If not, why isn’t it and make sure we let someone know.

And then we also have partnerships. We have a lot of partnerships with safety organisations that we work with to help us understand what’s going on in the real world. Because you know we’re a pretty big company now, over 20,000 people employed by Facebook, but we don’t have eyes and ears everywhere and it’s hard for us to understand the context of how our products are being used by the people in the real world. So the partnerships are very important.

And actually as you’ll hear from Sean shortly, we’re trying to use exactly the same approach, we also do a lot of training, either do training ourselves on use on how products work, why it is right to report things to us, what happens when you report, but also working with others who go directly into schools in particular so that they are furnished with that information. So it’s the combination of those things that we have learnt particularly the child safety, the safety of young people area, that we have brought that learning into this issue about political representatives. And how they can engage in a dialogue with people on Facebook which they are very keen to do, but also deal with when kind of heated discussion turns into abusive discussion and what they can do about it. And that’s where Sean and his team come in in terms of picking up that learning and thinking about ok how does that translate across to a world of usually adults, I mean some young people engage in these conversations, mainly talking about adults here, how do we ensure political dialogue but also can work properly.

And actually the one thing I didn’t mention was law enforcement. We also have relationships with law enforcement relating to parliamentarians. Emma will talk a bit about that.

PB: Thank you very, very much. Sean do you want to add something there?

SE: Sure, I can do a brief intro with who I am and what I do and what my team does. I also have some visuals we can go through during or after.

PB: Is there anything now, any gloss on what has just been said that you want to add immediately?

SE: So I run the politics and government outreach team for Europe, the Middle East and Africa. And I’ve been with the company a little over a year. Prior to that I worked for Twitter for a few years doing international elections, outreach. Before that the US congress right as social media started to become become a thing in the US congress. So as the resident social media expert on the committee, youngest person on the committee, really started to think about these issues with government officials, and kind of led to this role.

What my team does is focus on working to educate government officials, government agencies, elected officials, candidates, campaigns, anyone related to the government and political space, focus is having them understand what the platform is, facebook and the facebook family, who we are, what we do, how they can use it better to reach the people they are looking for. So if you are running for office, in the case of the UK election what we did is design a multi-faceted approach to this election, obviously it came up relatively quickly, but focus here is how can we work with the candidates how can we also work with the government and the new government, on understanding how to use Facebook well to reach the people they want to. We helped foster the two-way communication that happens on Facebook all the time.

What we did in this case for this election was go local and regional. So we trained people here in London but for the first time we actually went outside of London for an election and did eight different trainings on a local and regional scale, with over 5k candidates and campaigns and party officials. We hosted multiple webinars to help educate them not only on best practices and understanding new tools, as Facebook continues to evolve, every week we make a new innovative...

PB: Logic of what you are saying is that you do accept there is some additional responsibility during an election period? Because you got heavily involved, you changed, did new things.

SE: Absolutely, and it is also because there are more individuals involved. When you’ve got candidates involved, there is a chance that some will become government officials the day after the election so we want to make sure that everybody is on a level playing field and that they understand how to use the platform effectively and well and to the fullest extent they’re looking for. What we’re not are campaign advisors, my team does not go in there and say this is how you win an election. What we do is present the same level of best practices whether you’re running for a local council or whether you’re running for an MP and it’s basically just an extra set of eyes and hands, to say here’s an understanding of how the platform works, here’s some great examples of ways that you can be successful and most importantly talk to the votes and have them feel like they are better connected to you.

SM: Part of the training this time there were kind of some particular features on safety and haven’t done them previous elections

SE: Correct, and so while a lot of the training was generally focused on ‘Facebook 101’, we added on multiple pieces related to safety, whether how to report things quicker, the efforts that we’re taking as Simon mentioned we now have 4.5k people, that number will grow to 8k pretty soon, people that mainly review content, so it is educating candidates from around the country, so if they see something that bothers them, how do they flag that, how do they report that and what sort of steps do we take. Secondarily it’s other things that they can do to to keep account secure and prevent hackings and things like that. We’ve made multiple materials and [ ] we also pushed different products, eg if you were using Facebook during the election and you were a candidate you would have gotten a pop up saying here are steps to keep your account secure. Additionally we sent 3 different rounds of security and safety emails to every single candidate that we had contact for, so over 5000 again around the country, but we hit them 3 different times, just a gentle reminder of steps they could do to keep their account secure, ways they could report content that was inflammatory or suspicious content or difficult for them. And also advised on ways our our internal processes on ways we could handle it.

PB: Thank you very much. Jane.

JR: Thanks Paul. So social media providers have been criticised as you will be aware including in the debate in Parliament, what would Facebook say, how do you respond to that criticism that you have allowed a huge amount of abuse to be made directly and anonymously to people?

SM: So, there is no such thing as anonymity on Facebook - we have a real name policy, we’ve had that since the very beginning of Facebook. You have to use your real name on the service. It doesn’t mean people don’t try, much as in the UK we have a rule you can’t go above 70mph on the motorway, lots of people do. So people do try to open accounts in a fake name, and try and use that as a source of abuse, we know that internet trolls will try and use Facebook, because it’s a big community, if you want impact and you’re a troll, you can get onto Facebook and stick around then that can be quite helpful. But we do have teams that particularly focus on this, focus on authenticity. We really encourage people if ever they think an account, someone they are suspicious of, they think is fake then to tell us about it and then we can look into it. We can also require people to prove they are who they say they are.

SM: We are particularly concerned as you can imagine about impersonation. I guess especially during an election, someone might be impersonating a candidate and putting things out there that wouldn’t have been them, hence that’s some of the specialist advice.

In terms of the issue of responsibility, I don’t think there will ever be a time when I work for this company where politicians will say you’ve done enough. Or the media commentators, you’ve have done enough. You’ve done everything you can possibly do. They will always expect us to do more and we expect that.

I think the point at which we would not accept, is a suggestion that you should be responsible for everything that appears on Facebook as if you were a publisher. As if you were running the BBC’s website. That is not the nature of this service. This is a service which enables millions of people to have a voice that they’ve never had before; people to communicate with one another freely and in an environment where they are not expecting and indeed it would be completely wrong for their speech to be monitored. And that somebody is checking on all of their speech to make sure that it had not fallen foul of our rules let alone the law of the land. That is not the world we live in and I don’t think that’s a world that any of us want.

So it is not about being responsible for everything, but being responsible for saying do you have clear rules? Do you enable people, do you provide tools and make sure people know about those tools? Do you ensure that if somebody reports things, that those reports are reviewed and as far as you can, accurately and as quickly as possible, take action where people break the rules. We are absolutely happy that we should be held to account for living up to those conditions and we definitely can get better. We wouldn’t be investing in terms of community operation team as much as we are if we didn’t recognise we can faster and more accurate. We are also developing technology to help us on this.

We do not think that this leads to an end point at which we are then responsible for everything that is said and somehow can spot things without people telling us about it. That’s hard enough in areas eg even in an issue like nudity. Facebook doesn’t allow nudity. It’s not as easy as you might think to always spot nudity. And there are gradations and therefore it is really hard to do on that one.

When it comes to speech the contents are so difficult. Some people may find some content of speech offensive to them which others may find perfectly acceptable. So judging speech is much harder, but doesn’t mean we don’t try.

JR: Ok. So could you talk us through the process of how you monitor and deal with content that breaks your rules, policies and then as a subset of that, could you then go on to talk about the resources that are dedicated towards adjudicating cases that are reported to you.

SM: Yes, so I’ll talk about that more generally then perhaps Sean could talk about what happens when, for instance, during the most recent election in the UK, what happened if a candidate flagged something directly to his team say, or to my team.

So, do you have a Facebook account? I’d encourage you either to open one or to ask someone to show you this. Because it’s very straightforward to report things.

JR: I understand. I am completely clear as an ordinary user how one would do it but I want to hear it from Facebook’s point of view.

SM: So, any piece of content or account can be reported to us very simply, you do not have to go off to a help centre or fill in an email, you can report from the piece of content. There is a little drop down arrow on every piece of content. When somebody wants to report to us, they will get a pop up box where we will ask some questions to understand what the issue is. We do not have a big red button that you can press, because if that happened, we wouldn’t know what the issue was. Actually there is so much content and such a variation in how urgent an issue is for someone, that we want to ask questions in order to ensure that not only do we get the report to the right team and the right person, but also we are able to prioritise. So eg if somebody is reporting to us that they think somebody is suicidal, because of the content they are posting on Facebook, that is the kind of report we want to get to as quickly as possible because we can undo, help people in the real world in those situations, we have relationships with law enforcement that enables us to alert them to eg there is a young person in Mansfield, who is saying they are about to take some pills, we think they live here because of the information we have. And we can [produce?] examples of the police getting to that person, being able to help them.

JR: How many times in a year in England would that be operated or the UK?

SM: I’m afraid I don’t even know the number If we had I’m not sure we could share it but it’s a handful it’s not going to be....

JR: Could you share anonymised data with us?

SM: Not in terms of the number of reports of certain types, no. What I can say is that we do get millions of reports every week.

JM: How many in the UK, how many in England? How many would you have had in month of election in England?

SM: That’s not data we have.

JM: You don’t keep that data?

SM: We don’t have data that would tell us that?

JM: You don’t keep performance, you don’t do data reports on how many you’ve had in a particular period of what type of incident?

SM: No.

JM: How do you allocate resources then, how do you know how many people are needed to be reported to?

SM: We are looking at things at a global level usually on the basis of language rather than region. Because enormous numbers of people use Facebook in English across the world then our view is it doesn’t matter where you live or what your status is. If you are reporting to us that you are being bullied, and your report is in English, we want to get that to the team that understands English.

JM: So can you talk us through, say you have a suicidal teenager in Birmingham, England, you were saying that your team have first of all, you have a way of looking at things that need immediate action and that you have therefore a prioritisation team/process, and that you have a notification process to the relevant law enforcement authorities, why wouldn’t you have data that you are collecting, how do you know which law enforcement are recognising.

SM: It would depend on time of day. So If during the day our time, it is quite likely that someone in Dublin will be the first person to see that report. We have community operation centres in Dublin, in the US, in India. So we can cover whole world 24/7 and there is always someone available who can, not every language, may be some minority languages where we are not able, immediately, might then rely on a translation tool, but always for English, there is always someone, a specialist available to look at that. And then we have our separate, not that person, a separate law enforcement relationship outreach team that are available 24/7, we do have someone responsible for that for the UK who works with law enforcement units, but doesn’t need her to be on line and awake 24 hours a day. We have points of contact in every police authority in UK that we can reach out to with that information.

JR: So for the hypothetical teenage person in Birmingham, say they are posting online threats at 3am GMT, at what point are the law enforcement services notified?

SE: As quickly as possible. I can’t give you a definitive..

JM: Do you have benchmarks you are aiming for or performance.. You know, from end to end, from this happening it will be 5 hours or 3 hours or ...

SE: In the context of election, especially in the 72 hours around election day, we have certain tools we can turn on if a candidate is receiving threatening comments hypothetically, and that happened only, anything related to candidate urgent issues in that 72 hour period was a handful of times only, but we have dedicated support channels for big events things like that, will be responsive in 15 minutes.

SM: Just to be clear that is not all the time on every report, was because of the importance of the democratic event.

SE: That covers even if PM eg were locked out of Facebook account and was a time sensitive matter, all the way to something needing a very quick escalation.

JR: Going down the scale of immediate threat, what happens if it’s not life threatening, if it’s a threat of rape, how would that get dealt with, both in election and outside election period? How would you prioritise a rape threat against a candidate?

SM: In terms of the 72 hour period, it’s going to be treated very quickly, outside of that, I know you are keen for me to be definitive on that but I can’t give you a definitive answer, entirely depends on what else is going on. E.g. if there is a major unfortunate incident such as terrorism, we deploy teams and really focus on that to make sure we are looking out for intelligence on that either in private or in the media about the names of perpetrators or victims. Any praise for those acts because that is not allowed on Facebook. It will rather depend on what else is going on.

JR: Let’s assume it’s a quiet day at the office...

SM: There’s never a quiet day at the office...

JR: It’s a quiet day, not an election period but an MP has had really unpleasant stuff around rape put on facebook and she’s reported it to you. What would your timescale be, she’s reported it, her office has reported it, what would happen next, when does the prioritisation process that you talk about kick off, and then if you decide this sounds like a real threat, when do you then inform the law enforcement...

SM: Part of our training is, if it’s a real threat, don’t report to Facebook, report it to the police. We say to people report it to the police. We cannot stop you being raped, we can take down the content, but if you are really seriously worried about harm, you must report it to the police.

JR: But how quickly would you take down the content?

SM: As soon as as soon as someone looks at it and decides it’s problematic then take it down straight away. But we can’t guarantee, can’t tell you someone will definitely look at that within 15 minutes, depends what else is happening.

JR: It’s a quiet day at the office.

SM: No such thing as a quiet day for us.

JR. What is your range then?

SM: So we aim to get to every report within 48 hours, but most are much much less than that .

JR: And the rape threat stuff would be immediately taken down once you’ve looked at it?

SE: As soon as someone reports it on one of the tools on Facebook, it goes into a queue, and we are alerted, say the MP sends an email to one of us, we can escalate it ensure someone is looking at it. Every single issue is looked at in a 48 hour window.

JR: In terms of protected characteristics - gay MPs, black and ethnic minority MPs, even more so if both, and the intersectionality, what are you rules around what we call in Britain protected characteristics?

SM: These have rules that have nothing to do whether you’re a representative or not. We have clear rules about hate speech, We have defined protected categories that go beyond those in UK law, that say you cannot people on the basis of these protected characteristics, And that is irrespective of whether they are a representative or not. Happy to furnish you with those details. Something we do a lot of work around hate speech, don’t know how familiar you are with the work being done by the EU Commission on this to do with our companies. There is an EU hate speech code we’ve signed up to and so we deploy that irrespective or whether you are a political representative or not..

JR: Thank you. And what resources do you deploy to look at what happens in Britain on all the issues we’ve discussed.

SE: One of the main focuses of my job is outreach and training. One of the efforts we take is meeting with either large scale groups, full body of MPs or smaller groups on various specific trainings, not only on best practices for putting out your own content but how to engage when you have comments and content that you don’t like and one of the easiest things to do is to report it if it’s problematic, let us know and secondarily don’t engage with it. You want to highlight the quality content on the platform and use the opportunity to change the narrative a little bit, on one hand being proactive if you’re and MP and second hand making sure you are reporting things to us so we can look at it and take it down.

When it comes to the outreach efforts, we do routine trainings on certainly a quarterly basis with either guides like the ones you have in front of you, we have made multiple throughout the years and focused on very different subsets of MPs so the ones you’re talking about may encounter various specific issues, and have conversations with them on best practices and dealing with certain types of content. We also work a lot with third parties, outside groups NGOs etc, we worked specifically on a large campaign Europe-wide and hosted some kick off events in the UK on women in parliament in particular focused on efforts we can take to try to counteract some of the comments they get that might make a female MP feel uncomfortable. We hosted training seminars. We hosted luncheons in a lot of different places, and something we are going to extend.

SM: I wonder if it might be helpful to hear from Emma about the relationship with the Parliamentary police group.

EC: So the law enforcement team that Simon referenced earlier, we have connections and relationships with police forces around the country and around the world. We also have a strong relationship with the Parliamentary Liaison Team in the House. You’ll know that the Met Team based in Parliament, our head of that team who is based in London and has a UK law enforcement background herself, has done training with them, has done 1 to 1 work with them around how we deal with different kinds of crime that might be perpetrated on the platform against MPs, what constitutes a crime that might be reported, what constitutes content that might be taken down. And we have a ‘government casework ‘channel’ which is with this particular team in parliament and with trusted NGO partners around things they have seen that they can escalate more quickly to us, so the review skips a certain, couple of steps so gets reviewed by humans immediately. If a police officer in parliament has had some content reported to them by an MP, they are trained in both law enforcement by their very profession but in our standards too, they can very quickly say yes, this needs to come down immediately and they escalate it. Or equally, they are on the ground saying, yes I can understand why this is distressing but it’s either (a) not illegal but could breach standards of Facebook, so let’s get this escalated; or this is not illegal and probably wouldn’t breach standards so let’s find a way that we can handle it here in the House. So that is a relationship we have with them and that’s something that continues and they have a very open channel with us. Not a case of a law enforcement team presenting and walking away, that’s an open feedback channel and across all subject matter that you might think of, hate speech.

SM: They can also request data from us. For law enforcement around the world, we have an access channel which enables them to request data from us if they believe a crime has been committed on our platform, something the UK police make regular use of, we provide public information on this, we report every 6 months on the number of requests we’ve received from law enforcement around the world and the UK is usually in the top 3 or 4. Now I don’t know how many were to do with parliamentarians, but I’m sure if you asked them they could tell you.

JR: Thank you. How do you respond to criticism in the wider media and we have heard evidence on that Facebook can be slow to remove posts even when courts have taken a view. So for eg, some evidence is that not an MP, someone else in public life, a Police Crime Commissioner’s [redacted] view was that Facebook and others were slow to respond to take material down.

SM: I’m afraid I don’t know about that individual. We certainly are aware of occasions when people feel we’ve been too slow or have made the wrong call. When you are making millions of decisions like this every week, no matter how good your training is, how much you really try to get it right every time, you can’t always get it every right. So one of the reasons we appreciate having channels like the one with parliamentary authorities and campaign parties who let us know when something has gone wrong, we have made the wrong call. In terms of being too slow, we are putting more resources into it, an indication we know we need to invest more in this area and that’s exactly what we’re doing.

JR: My next question, you hear a lot directly notified, you know about, well informed about what’s going on in this area in election and Scottish referendum, what’s your connection with Facebook board and Facebook decision makers in America, what is the governance arrangement?

SM: So everyone in the UK, their version of Facebook is provided by Facebook Ireland, and therefore when it comes to things like data protection, data privacy, the European framework as promulgated through Irish data protection legislation applies here. When it comes to the issues that you’re focused on which is to do with rules about what is and not allowed, those are global rules set out in our community standards that apply everywhere equally so irrespective of local law we apply the same rules on what and what is not allowed on Facebook.

I mentioned earlier about nudity, there are some countries that think it wrong that we don’t allow nudity, that we should because that’s something they are perfectly comfortable with but you can imagine the countries I am talking about. There are others who think we should be more strict and we shouldn’t allow pictures of women in swimming costumes. Right, so one of the reasons we apply the same rules everywhere.

In terms of governance when it comes to matters of political speech, where governments in particular want us to take down political speech, those issues tend to be escalated to the US and are taken by our, she’s a public figure, so happy to name her, person who runs content policy for us is someone called Monika Bickert[[1]](#footnote-0), you may have heard her name spoken to day, she is with the PM at events at the UN General Assembly. She is ultimately the person in charge of the application of our policies. Sometimes, things get escalated above her, particularly decisions about political speech and where we are being put under pressure either to take it down or our service will be blocked. She is not on the board but she is an extremely senior executive.

We never have that issue in the UK. The UK government may sometimes think that we have not taken down content that they think we should, but they have never threatened us with being blocked. But in some of the other countries that I deal with, that is a very regular occurrence That is why we have the governance structure that we do, that decisions are not made here, We do not make decisions in the UK about what content is and is not allowed on Facebook. Those decisions are taken by people in Dublin, Hyderabad or California depending on what team is awake and where decisions are made. Escalations always go the person in charge of our content globally.

EC: Is it worth talking a little bit about your role in a local context for that? So whilst it gets escalated to Monika, actually the importance of having people on the ground.

SM: Thanks Emma. One of one of issues is that sometimes context matters. Less so in UK, but certainly in other countries I am responsible for, there are certain slurs which people may not be aware of, particularly in other languages, trying to understand is it hate speech or not hate speech, a particular word, and that is often where the local team like ourselves, our insights and advice can be helpful to those global teams that are making decisions about whether content is or is not allowed on the platform. Those are the marginal cases, but you can imagine when you are dealing with millions of reports, there are lots of marginal cases every week where the judgements are having to be made. But to be absolutely clear, we provide advice but don’t decide.

JR: Thanks, on resources, you have mentioned that Facebook is going to be putting in more resources into this area. What scale are those resources going to be? I couldn't’ get a sense of what resources there are currently, you mentioned India and Ireland?

SM: We announced earlier this year 3,500 more people in community operations and that was on top of current 4000 already employed. We are now at 4,500, so that’s an extra 3000 coming and the plan is to get them all in this year. So aiming for 7,500 overall. Our total number of employees at the moment is just over 20,000. It’s a very large part of our people resources are focused on community operations.

DG: Thank you. Sorry to take us backwards a little bit, just wanted a point of clarification. We were discussing protected categories… there are some things that we’ve received evidence from Parliamentary candidates where things have appeared on Facebook that they believe should have been taken down that haven’t been. And we’ve read a *ProPubllica* report, I’m sure you’re aware of it, about cross-cutting protected categories, perhaps you could explain that to us a little bit so that we can be clear when we are writing our section on that.

SM: Yes. It’s a tricky one but let me try and see if I can explain it. I can understand it may feel rather odd. So I think the specific example was this notion whether black children are a protected category given that black men are or white men are. Age is not a protected category, and therefore children and old people or middle aged people are not protected categories. You can say on Facebook I hate old people or I hate kids, that content is fine. But you cannot say I hate black people. One of the tricky thing becomes when those things are combined and therefore how our rules apply. Because I don’t want to misspeak, I would quite like to go back on that particular example because it could well be one where we have reflected on it further. And actually after all this wasn’t a decision, this was about a leaked document which was a training manual to try to help our agents who are making these decisions to try to understand the nuance of what happens when someone isn’t just described in one way by someone whereas a combination of characteristics is used to describe someone in a hateful way which contains some things which are protected and some things which are not.

So political beliefs are not protected. You can actually say I hate people who are voting for Jeremy Corbyn. You can say that on Facebook and you can say you hate Labour supporters. And I think we’d all agree that is part of the political dialogue. But if you say I hate women who are voting for Jeremy Corbyn, is that ok or not. That is a highly nuanced area and I’d be fascinated to see, what do you think abou that? How can you enable people to use protected characteristics in the context of what people might believe or might be thinking in a way which still allows for discourse but tries to tackle the problem of hate speech. It’s a tricky area.

DG: So you would be able to send us some more information on what your current training is around those protected categories and combinations.

SM: We can look into whether we can provide you with any of our training manuals. I want to manage your expectations around that. It may not be possible to do that.

DG: If not the training manuals, what the existing standards are.

SM: Sure.

DG: And talking about context, you mentioned previously about developing technology in this area, wondering what are you doing to improve the automated monitoring of content? And what your medium and long-term ambitions are in that area?

SM: So this is an area in which there Is enormous promise but we are very cautious in being too optimistic about how quickly that promise might be achieved and how accurate it will be. We are absolutely doing a lot of work, investing a lot of resources in trying to get better at potentially not wasting people’s time. So most of the content reported to us does not infringe our terms. Classic example is when there is a football match involving Chelsea and Tottenham or Galatasaray and ... But often when you get local derbies, you get huge volumes in reports, people will find all kind of things that have been said, and we have to absolutely have to look at them because there could be something in there which is serious, but it means an awful lot of wasted time. And what we want to try and do is cut out the waste so that generally most times when a human reviews something it is a problematic post or piece of content which will result in an action. Because everytime there’s no action, it’s a waste of their time.

So there are some areas it’s easier to do this on than others and actually we are getting much better at doing this around images. This partly comes out of work we’ve done on accessibility. Facebook, Instagram are predominantly visual media. If you are visually impaired, that can be very difficult so one of the things we are doing is using AI to help the visually impaired have a great experience on Facebook. Doesn’t mean that somebody else will look at the image for them, but the AI will be able to tell them that this is an image posted by or tell them who’s in the photo, what’s in it etc because of AI. So we can use that as well to try and identify nudity without someone having to sit there, looking at all the stuff that’s being reported as nudity and saying yes no, yes no. Language is about the hardest thing because of this issue of context. The number of times people will say kill, die, etc people say that a lot, but you know “I could kill a cup of tea” so the notion that we look at the word kill, to look at all the posts involving ‘kill’ would be a massive waste of time. So it’s the hardest area but nonetheless it doesn’t mean we are not going to try.

We will try and see what can you do to surface content that is not being reported in order to see whether or not it’s infringing our rules.

I would say, that in this area of personal abuse, bullying if you like, having the person who is feeling bullied telling us about it is always going to be much more helpful than having a third party doing it. If you don’t mind, I’ll give you an example of this. In Ireland we once had a headteacher who reported to us that an image of one of their teachers was bullying him, this was an image of a teacher and under it, someone had put ‘gay’. And that we should take it down. We would not take that down until that person reported to us because saying someone is gay is not a form of abuse. That person may or may not be gay, there may or may not be bothered about the fact that somebody has put their picture up and put the word gay up under it, we need that person to tell us this is abusing me. So those areas of context, how does this make you feel are incredibly hard to do with technology. Doesn’t mean we won’t try and try to learn as we go through this but I do want to manage expectations about how feasible that is to think that this will be solved by technology.

DG: But that does require that Parliamentary candidates to have read the stuff that is intimidatory.

SM: Or their campaign team or

DG: And so you will be aware of other platforms for example hiding the comments or posts that they think are likely to be intimidatory which then people can read if they choose to. Is that something you would be looking into in the future?

SE: We’re constantly looking at ways to make it just a little bit easier for candidates, we’re receptive to this sort of conversation. When it comes to comments in particular, there are options, they can hide or delete certain comments. And it would also delete comments under the thread which could be difficult when you’re looking at a political issue, but yes, they have the ability to....

SM: What about the profanity blocker?

SE: Actually yes you have the ability to essentially block certain keywords from appearing on your page, basically blacklisting them, and most of that would fall under profanity [?].

DG: Thank you. Do you see opportunities to work with other social media companies on this kind of automated or machine learning area and are you taking steps to do that?

SM: There is a lot of work in the area of terrorism and extremism, being talked about in New York today. When for instance, one of the big issues is, when a new piece of propaganda comes out from a terrorist organisation and they try to distribute it through all the different platforms, the first time it appears on one of our services, if we can kind of spot that, reverse what they are trying to do and then we have ‘hashing’ - which is that we kind of code that piece of a content so that other people can spot when there is an attempt to seed it on other platforms. We share those hashes. We have created a databank of those hashes of kind of extremist propaganda in order to ensure that those who would support ISIS and Al Qaeda for instance, when they try and seed that in networks they are unable to do so. So it is a disruptive mechanism. That’s a classic area where we co-operate.

SE: In terms of elections, we’ve got the same sort of channels open - routinely done work with Google and Twitter proactively around things like voter education, voter efficacy, candidate understanding and education around this and also working with them as soon as we come across bad [actors?], making sure those lines of communication are open.

PB: Can we come back to the very interesting example you give about the Irish case and the use of the word ‘gay’. Let’s suppose you talked to the teacher involved and he said it’s really upsetting me, it’s not an act of self-affirmation or whatever, it’s really upsetting me. What happens then, what we’re really interested in is very obvious to a lot of people who are subject to this kind of hassle, and do not report it to the police. What happens in terms of illegal behavior? Let’s assume now we’ve passed the test and the person involved says I don’t like it. What then, what steps do you take to ensure those kinds of cases can be easily referred to the police and the relevant authorities?

SM: I mean actually if we see criminal activity on our service, particularly the most serious then we can and do alert the authorities, but most of the time it is the police coming to us. Because what’s happened is someone has seen something, they have gone to the police and then because the police have our colleague who is our representative [name redacted], they train police forces all over the country so they have a single point of contact with Facebook. They know them so therefore they can come to them and ask for information to help the authorities.

PB: Now the other thing that we hear, I’m not quite sure with how much accuracy, is the sense that US agencies get privileged access in these difficult areas. You’ve recently acquired What’s App which is an encrypted messaging service, is that the case in terms of difficulties that might occur in that sort of context or is that something that is something that people say that isn’t necessarily true?

SM: I think this would be a good one for you to raise with the Home Office. There are international agreements around the sharing of data. So there are number of different things going on here. One is that the US has a law that says you cannot share content with overseas governments/authorities unless there is a relevant order in the US courts. So we are not allowed to share content. There are two different things: the data about an account - the name, address, phone number, an IP address we can provide. What we can’t do is provide content unless it is an emergency because of this US law. But there are relationships between US and UK authorities allow them to ask for it from the US authorities and there is also an active discussion between the Home Office and DOJ around a bilateral agreement between the US and the UK which would allow us to disclose content directly to the UK authorities.

We would be very supportive of that, it just needs to be agreed between the governments. So the answer is yes, the US authorities, it is more straightforward for them to get content but not because of something we have done. It’s about this international agreement and US law when it comes to sharing of content.

PB: Thank you very much.

JR: Could you talk to us a bit more about anonymity online, appearing to perpetrate the problem of online intimidation and obviously you don’t permit anonymous accounts, what do you do about fake not real personal accounts, how quickly can you spot them and what do you do about them?

SE: So there’s a few different things. One is on the reactive side and one is on the proactive especially let’s look at it through the context of the election. Reactively we work and my team in particular works with everyone when it comes to government and political folks. If they come across an account or somebody comes across an account that is say Theresa May but spelt a little bit differently but looks the exact same, that’s a violation of our terms. So as soon as we are made aware of that, we act very quickly to remove that. It is put into a high priority queue because you know you could have that account talking about things that are related to policy and people just assume that it’s real. So we work very, very quickly and carefully to make sure those are removed from the platform. Additionally we have proactive efforts, which if you see the little blue checks marks by certain accounts, those are the ones that are verified pages, verified accounts, so those are the real accounts.

In the context of the election, we put out brand new tools not previously utilised to connect local voters around the UK with their newly elected officials. And we worked with the various groups internally in the government and also third parties to make sure we had the accurate candidates and elected officials. As soon as they got elected on election on election night we were able then to push to citizens all around the UK the accurate accounts of people they could follow and connect with their newly elected representatives.

So on the reactive side, we taken things, we have different procedures in place to move on quickly, and on the proactive side we try and find ways to make it easier to find your elected officials and then also to connect with them.

SM: And just to be clear, there are a range, when someone reports to us that an account is fake, we don’t immediately take it down, because we also see quite a lot of people trying to as it were to attack someone else by claiming that they are not real. So we do give people an opportunity to prove that they are who they say they are. And some people have quite unusual names. So you can’t do this on the basis that this doesn’t seem a real name. So this is something where, and you can imagine where somebody has built up a bit of a following and they’ve got a rather big account, to lose access to their Facebook account is a big deal. So it’s not something we take lightly.

JR: So how long would that take that sort of due diligence?

SM: It will depend, you know, so we have a process where we will ask people to prove their identity. They have to upload identity documents, and then we have an authenticity process? [ ]. It will entirely depend on how quickly they upload the documents. But we also have a checkpoint, we can say you haven’t lost your account..

JR: Triangulation thing when you say check point?

SM: No checkpoint means you are not able to access you account for a period until you’ve proved that you are who you say you are. So it doesn’t mean we’ve deleted the account. Or we could just prevent them from uploading for a period and that’s one of the things that happens when we find someone’s breached our terms. We don’t automatically take an account down for breaching our terms. We have graduations of sanctions which can mean you’re not allowed to post on your account for a week, or you’t not allowed to upload photos because you’re abusing your photo tool. Something like that.

JR: OK. Did you notice that was much of a problem during the 2017 elections (impersonations)?

SE: No not outside of the norm.

JR: OK, that’s helpful. So slightly different point, how do you respond to calls for legislative changes on online hate speech and intimidation. I was thinking of Germany’s recent legislation requiring clearly illegal material to be taken down within 24 hours of it being reported?

SM: When it comes to the German legislation, we recognise particularly in the context of that country, because of its history and more recent history in intake of lots of refugees, we recognise that parliamentarians have taken that decision to implement that law in good faith and we are working with the relevant authorities to understand how it will actually work in practice. That’s really not clear. I don’t know how close you have looked at the law, but my understanding from my German colleagues is that it is far from clear how this will actually work in practice and therefore what we should do about it.

Our position is we would much rather when there are genuine, and there are genuine attitudes that concern, let’s try and work with parliamentarians, with governments, with NGOs and all the other relevant parties and with other companies to try and address the problem, such that parliamentarians don’t feel that they have to regulate. So it’s not don’t regulate us, it’s let’s try and address the problem so you don’t feel you have to. And if we fail, as in if we are unable to convince parliamentarians that we’ve in terms of a particular issue that our interests are aligned and that we are doing lots of things to address them and are open to doing more if there are some other ideas, if they decide after all that there are still things that need legislating, it is clearly their call and we respect the democratic process.

PB: That really is very helpful to us. Want to ask you a question that is a bit unfair. Is there anything that you think springs to mind immediately that could be done to protect parliamentary candidates? We have on the whole come to the conclusion, this committee, that there was a special problem at the last election. Not everyone quite agrees by the way, in terms of the communications we’ve received. But, on the whole, the balance of the evidence we’ve received is that there was a special problem and people had to put up with things that they shouldn’t have to put up with and a lot of this was occurring online. What would you do if you were us?

SM: Our perspective, is that government couldn’t call snap elections because as Sean can attest, one of the issues we had is we had to employ training and resources at a faster speed than we would have liked and it meant we were simply unable to get to some of the candidates so that they were unaware of our support that we provide and the tools we have. Now, I know that’s not within your purview, but something about if you’ve got a reasonable length of time to know the election’s coming, we can certainly do a lot more work, work with more partners, work with more agents and campaign teams.

PB: That’s a useful point.

SM: It was certainly a factor for us.

SE: We had very little time to ramp up an operation that we wanted to be very proactive outside of just Westminster and Whitehall. We wanted to find opportunities to go more regional and local and that’s tough to do when you’re in a very compressed time frame. The fact that we were able to connect with nearly 5000 candidates was still pretty impressive. I’m looking forward to build those relationships outside of London, more regionally and locally and have opportunities for more face-to-face conversations. We did a lot of that as we stated but we also did a lot via webinar, a lot via email, but having the face-to-face conversations with various candidates and elected officials at all levels is something that I know from my side, my team is going to focus on very heavily.

PB: I’m gathering from this you wouldn’t have any objection to a deepening of dialogue with government and political parties about what could be done to deal with these problems of online intimidation?

SM: Absolutely, we are always, dialogue in these things is always important. We certainly found that in the wider child safety space. It’s that combination of being clear about the rules, what’s allowed, what’s not allowed, training and then deploying our resources of all different types and the more dialogue we have including the better.

PB: And in terms of working with the Parliamentary Police who are looking at these questions, you will continue to be working with them. Is there anything you want to add on that?

EC: So in terms of continuing the conversation, everything that we’ve said already stands and Sean’s team have good plans about what they want to do in between elections. This doesn’t just stop when an election is over. But a lot of work around that. But to build on Simon’s point, what we’re really keen to do is have really meaningful conversations with people who have been through this to get to the nub of the issue. So that we can come to solutions. I think what we get at the minute is a wave of general descriptions of abuse, and maybe delving into what kind of abuse, is it gendered abuse, is it politically-divisive abuse. What the nature of the abuse might be is something we quite want to do.

SM: And it’s one of the reasons why we’re very supportive of the Recl@im the Internet initiative that Yvette Cooper and other Parliamentarians initiated. We’ve supported that work and been both in the background, providing advice about how we approach this but certainly some of the resources you see here particular focused. We know there has been a very particular focus about female MPs, but also there are certain groups we’ve not seen before in the UK political scene, in particular Momentum that have been associated with this kind of abuse. So we also want to really emphasise we do not think this is about our companies getting this right. There are lots of things that political parties need to address, that the media need to address, that the police need to address in order to o ensure there is a collective ownership of how we an try to address this recognising that there is also this wider issue about how people engage with each other. So how do we as citizens, engage online, on public transport, in the football stadium, wherever we are, how do we engage with one another. And Facebook isn’t a special place like that. People I’m afraid do sometimes engage in ways that go beyond robust and heated dialogue into abuse. We wish that weren’t so but I’m afraid it is and we need to just make sure that when it does happen, people know what they can do about it.

PB: Is there a particular demography you see which is not people of my age, you know, that’s also a factor in tone I think?

SM: I’ve never seen that data, you may be right. I’ve never seen data about is it younger people or Southerners, or Lancastrians, I’ve never seen data like that.

Emma: I just want to very quickly close the point about Recl@im the Internet just to touch on the fact that what you have in front of you is a very generic version of what we’ve done on safety. Something that we have been considering further to your point about considering the conversation with Parliamentarians, is probing how useful something much more detailed and specific would be so that Sean’s team and our team can work together a little bit on what more information, resources there could be that go beyond general women, but female MPs, or MPs in general. We have an example of that, I couldn’t find a hard copy today I’m sorry, of something we’ve done for journalists for example who are in a similar public position and get similar messages. So I’ll get the digital version, it goes deeper than this. We are wanting to start conversations about whether that’s useful.

JR: In terms of, obviously we’re talking to yourselves and Twitter and seeing Google tomorrow, I think it’s tomorrow, one of the things if you’re a candidate or some of the people who have given us evidence who are in public life, like broadcasters and journalists or local councillors, say that it’s the combination of the opportunities of abuse they receive from Facebook and Twitter and others. So is there connectivity in terms of dialogue at the most senior levels for example between Facebook and Twitter on these issues?

SM: Not about individual accounts because we can’t talk about people’s individual accounts.

JR: I meant in terms of policy which might lead to connectivity. Is there something which is a Twitter account which is spewing out 1000s of abuse say to Diane Abbott and also there is activity on Facebook about Diane Abbott for example?

SM: Well, not explicitly like that in the sense of, if there’s an account like that doing something on Twitter, Twitter would not be allowed to share with us information about who that individual is so that we can as it were address their activity on Facebook. They are not allowed to share that and nor are we because we can only share people’s information with their permission. The police could link those up of course by asking each of us for information. But certainly at the policy level, on public policy we don’t compete; we compete for advertising, people’s ‘eyeballs’, we do not compete on public policy, we are very aligned on this and this is an area where we all have an interest in supporting the democratic process, allowing people the free speech but tackling abuse.

DG: Just a quick point regarding referrals to the authorities/police, not just where the authorities request information, but how you enable users to go through the process of reporting something to the police?

SM: We don’t, there isn’t a mechanism for reporting things to the police via Facebook.

DG: Do you feel at the moment your guidance on how to report something to the police and what kind of information the police might need from the post, do you feel that is sufficient at the moment?

SM: That’s a great question and I have to say I’ve not looked at that more recently. Certainly, when it comes to locally produced material like this, these are quite generic, but we’ve certainly worked with safety organisations to produce specific safety advice for say young people in the UK which fully included information about where they can get help. But say you go to the Facebook help centre, there’s a help centre which is available for 2 billion people across the planet, so having something that’s kind of specific about what number do you call to call the police. I guess I would suggest that most people in most countries do know the number to call to call the police. But it’s an interesting question and we’re happy to have a look and see if there’s something we’re missing. I would suggest when it comes to the issue of parliamentary candidates, that’s a different matter. If there’s something else we could be doing in our collateral about this and in our training to remind people that if something’s happening on Facebook that you think is criminal, then call the police then we’re happy to look at that. We can happily review it.

DG: For example we’ve heard from the police that people send screen shots as opposed to URLs of abusive content and it’s much more difficult for them to track that down. And that’s the kind of guidance that perhaps users could receive at the level when they’re reporting something to you.

SM: Happy to look at that.

PB: We want to thank you very much for the detailed way you’ve answered the questions this morning. We would be grateful to see the thing on journalists that you’ve mentioned. As I said at the beginning, if there’s anything else that you want to add to anything you’ve said this morning, we’d be very grateful, just contact us. We have until just before Christmas when we will produce this report. Although technically we stopped taking evidence last Friday, actually I do think it’s useful to say to people we have still got ears. So thank you very much indeed.

SM: Happy if there are follow up questions.

CSPL Secretariat

September 2017

1. Head of Facebook Global Policy Management. [↑](#footnote-ref-0)